NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EFFICACY OF IEEE 802.16 BASED RADIO-WAN (WIDE AREA NETWORKS) IN SUPPLEMENTING SATELLITE COMMUNICATIONS IN AN INTRA-BATTLEGROUP AND AMPHIBIOUS TACTICAL NETWORK

by

William E. Wren

September 2007

Thesis Advisor:	Rex Buddenberg
Second Reader:	Carl Oros

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2007	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE: Efficacy of IEEE 802.16 Based Radio-WAN (Wide Area Networks) in Supplementing Satellite Communications in an Intra-Battlegroup and Amphibious Tactical Network	**5. FUNDING NUMBERS**
6. AUTHOR(S) William E. Wren	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT *(maximum 200 words)*

The concept of Network Centric Warfare (NCW) promises to revolutionize the manner in which warfare and military operations are planned and executed. While many information systems are in development, or currently in production, which seize on the NCW initiative with the goal of enabling United States and coalition military to share information on a scale never before seen, the pace of application development has outpaced that of transmission media development. As information systems become more complex and the amount of information that must be exchanged between units on every level of the military hierarchy has increased, units on the tactical edge that must rely on satellite communications or low bandwidth radio communications will increasingly find themselves on the outside of NCW environment looking in.

This research effort will demonstrate the increasing communication needs of naval units within a battlegroup and amphibious distributed operations environment and discuss the significant limitations that these units face with respect to bandwidth and how that affects their ability to efficiently transfer information. This research will also propose a tactical network based on IEEE Standard 802.16 wireless technology as a means of creating a tactical network for use within the battlegroup reducing the reliance on satellites communications to facilitate all of the communications needs of the units. Based on previous research efforts and field experimentation conducted for this research effort, recommendations are also made for improving the protocols contained in IEEE Standard 802.16 to make them even more suitable for use in a tactical environment, in addition to recommended research of support hardware for wireless communications based on IEEE Std 802.16.

14. SUBJECT TERMS IEEE 802.16, NCW, Network Centric Warfare, Tactical Networking, Intra-Battlegroup Communications	**15. NUMBER OF PAGES** 151
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

EFFICACY OF IEEE 802.16 BASED RADIO-WAN (WIDE AREA NETWORKS) IN SUPPLEMENTING SATELLITE COMMUNICATIONS IN AN INTRA-BATTLEGROUP AND AMPHIBIOUS TACTICAL NETWORK

William E. Wren
Lieutenant Commander, United States Navy
B.S., Oregon State University, 1997

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2007

Author: William E. Wren

Approved by: Rex Buddenberg
Thesis Advisor

Carl Oros
Second Reader

Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The concept of Network Centric Warfare (NCW) promises to revolutionize the manner in which warfare and military operations are planned and executed. While many information systems are in development, or currently in production, which seize on the NCW initiative with the goal of enabling United States and coalition military to share information on a scale never before seen, the pace of application development has outpaced that of transmission media development. As information systems become more complex and the amount of information that must be exchanged between units on every level of the military hierarchy has increased, units on the tactical edge that must rely on satellite communications or low bandwidth radio communications will increasingly find themselves on the outside of NCW environment looking in.

This research effort will demonstrate the increasing communication needs of naval units within a battlegroup and amphibious distributed operations environment and discuss the significant limitations that these units face with respect to bandwidth and how that affects their ability to efficiently transfer information. This research will also propose a tactical network based on IEEE Standard 802.16 wireless technology as a means of creating a tactical network for use within the battlegroup reducing the reliance on satellites communications to facilitate all of the communications needs of the units. Based on previous research efforts and field experimentation conducted for this research effort, recommendations are also made for improving the protocols contained in IEEE Standard 802.16 to make them even more suitable for use in a tactical environment, in addition to recommended research of support hardware for wireless communications based on IEEE Std 802.16.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AIS	Automated Identification System
BS	Base Station
C4ISR	Command, Control, Computers, and Communications for Intelligence Surveillance, and Reconnaissance
CHD	Complex Humanitarian Disasters
COASTS	Coalition Operating Area Surveillance and Targeting System
COP	Common Operating Picture
DO	Distributed Operations
DoD	Department of Defense
DRDO	Defense Research Development Organization
DSL	Digital Subscriber lines
EPLRS	Enhanced Position Location Systems
ESA	Electronic Steerable Antenna
FHL	Fort Hunter-Ligget
GMII	Global Maritime Intelligence Initiative
GPS	Global Positioning System
GWOT	Global War on Terrorism
HFN	Hastily Formed Networks
IEEE	Institute of Electrical and Electronics Engineers
IIFC	Inter-agency Intelligence and Fusion center

IMO	International Maritime Organization
ISR	Intelligence, surveillance, and reconnaissance
JFMCC	Joint Force Maritime Component Command
LAN	Local area Network
LOS	Line of sight
MAC	Media Access Layer
MDA	Maritime Domain Awareness
MIO	Maritime Interdiction Operations
NCW	Network-centric warfare
NECC	Naval Expeditionary Combat Command
NGO	Non-governmental Organizations
NLOS	Non-line of Sight
NORM	NAK-only reliable multicast
NPS	Naval Postgraduate School
OEF	Operation Enduring Freedom
OFDM	Orthogonal Frequency Division Multiplexing
OIF	Operation Iraqi Freedom
OSPF	Open Shortest Path First
OTM	On the move
PHY	Physical Layer
PSI	Proliferation Security Initiative

PtMP	Point to Multi-point
PtP	Point to Point
QDR	Quadrennial Defense Report
QoS	Quality of Service
RAAF	Royal Australian Air Force
RAN	Royal Australian Navy
SINGARS	Single Channel Air-Ground Radios Systems
SNMP	Simple Network Management Protocol
STOM	Ship to Objective Maneuver
TCP	Transmission Control Protocol
TNT	Tactical Network Topology
U.S.	United States
USCG	United States Coast Guard
USMC	United States Marine Corps
USN	United States Navy
USPACOM	United States Pacific Command
USSOCOM	United States Special Operations Command
WAN	Wide area network
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGEMENTS

The process of researching and writing a thesis is a difficult task and cannot be done without help, guidance and experience of advisors, counselors, and family. I would like to express my greatest appreciation to all of those at the Naval Postgraduate School who assisted me in my research efforts. Thanking everyone individually would be a paper in and of itself. I would like to specifically thank those below. Without their guidance and support, none of my efforts would have been possible:

LtCol Carl Oros, for providing endless hours of conversation, poignant guidance, mentorship, challenges, and the chance explore.

Rex Buddenberg, for continually expanding my horizons, providing more Coast Guard anecdotes than can be counted, and for helping me to keep my focus regardless of the environment around me.

Brian Steckler, for helping to stir my interesting mobile communications and providing me virtually any assistance that I needed during my efforts.

Bob Broadston, for providing continuous "sanity checks" and for helping to give me the means to make this research possible.

Dr. Francis Shoup, for believing in me and my ideas of "crossing rice bowls".

Dr. Alex Bordetski and Eugene Borakov, for providing me a venue for my experiments and helping me laugh and see the bright side of things when experiments fell apart.

Maj Brett Laboo, Royal Australian Army, for acting as the "Australian Translator" during TALISMAN SABER 2007. Without his help, humor, resourcefulness, and knowledge the NPS Communications Team would still be lost in Australia.

My family and friends, for keeping me sane (somewhat) throughout my time at NPS.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

When the Advanced Research Projects Agency (ARPA) first interconnected a small number of sites together in 1969[1] in an attempt to create a flexible and resilient means of communications in the event of a nuclear attack by the former Soviet Union against the United States, they had no idea that forty years later their creation would bind the world in a virtual network accessible in every country by billions of people (Kleinrock 2002). Their creation would become the lifeblood for millions of people, spawn new industries, and enable an information sharing revolution on a scale never seen in human history. Though turned over to civilian control, the military has continued to seek ways to harness the power of the internet to assist in war fighting and bring the power of information to every level of the military.

Network Centric Warfare (NCW) is the current embodiment of the Department of Defenses' effort to harness the power of information technology to share information among geographically dispersed forces. This concept enables commanders on all levels to request and obtain critical information regarding their battlespace space in order to more effectively employ their forces by achieving information superiority (Alberts et al. 7). Simply put the NCW concept calls for everyone to have immediate access to information contained on a multitude of platforms and have the ability to communicate with any one at any time for the purpose of planning and executing military operations. The concept of NCW can also be viewed as an attempt to harness Moore's Law and Metcalfe's Laws.

Moore's Law, first proposed by Intel co-founder Gordon Moore in 1965, basically states that the computational power of a computer will double on average of every two years. The concept of NCW attempts to harness that computational power that is ever increasing at ever decreasing costs to benefit the warfighter and make computational devices ubiquitous on every level of war fighting. However, individual computational

[1] The network would later become known as ARPANET.

devices are of little use if they are not connected to each other by some means; a car is of little use if there is no road to drive it on. In order to make information ubiquitous on the battlefield, NCW conceptually calls for all of the computational devices to be interconnected bringing an intrinsic value to the network described by Metcalfe's Law (Alberts et al., 91).

While Moore's Law deals with the exponential increase in computational power, Metcalfe's Law focuses on the intrinsic value of a network. Metcalfe's Law, first proposed by Robert Metcalfe in 1970, states that value of a telecommunications network is proportional to the square of the number of users of the system. This means that, assuming every user contributes equally, the intrinsic value of a network will continually increase. The NCW concept seeks to harness this concept as well by creating a inter-networked battleforce with the capability to communicate with every node in the network and freely and reliably share information allowing for the battle force to gain information superiority over any adversary (Alberts et al 97).

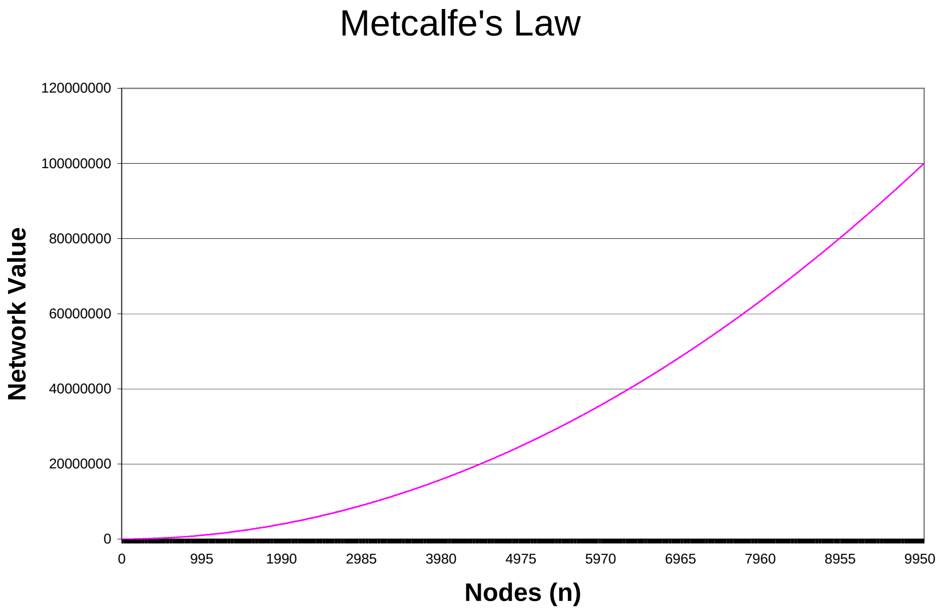


Figure 1 Metcalfe's Law.

Today, systems built with the concept of NCW and joint warfare are quickly approaching production versions ready for fleet and field trials in actual combat scenarios. If successful, these systems have the potential to revolutionize the manner in which the United States conducts warfare. Due to the growth predictions of Moore and the networking value predictions of Metcalfe, the military will soon operate in a battle field unbounded by geographic constraints. However, connection to this network of information systems is currently a problem and has the potential to remain a problem for field units into the future.

System initiatives such as the Global Information Grid (GIG) Bandwidth Expansion (BE) have created one of the most capable terrestrial global networks in the world with bandwidth up to OC-192 (10 Gbps) available to units capable of connecting directly into the GIG (DISA website). However, field and mobile units must connect to the GIG using satellite communication systems that pre-date the digital revolution, or were designed and deployed prior to the military's wide adoption of and reliance on IP-based communications. The military's reliance on satellite communications to connect dispersed units into the GIG has created a telecommunications "bottleneck" that threatens to limits those units participation in a fully NCW oriented environment.

While new satellite communication systems are being designed which are capable of bandwidths up to 10 Mbps per unit, Moore's Law states that these systems will quickly become outdated and incapable of providing the bandwidth necessary to support remote units. Additionally, in order to provide every unit, down to the foot solider, satellite communications, this would entail each one of those units to possess a satellite receiver. While this is a potential viable solution for ships and company level detachments, it is not a viable solution for foot soldiers. In order to reduce the military's reliance on satellite communications while enabling units to participate in a fully NCW oriented environment is a tactical network based on wireless communications. The military must harness capabilities available to the commercial sector to economically provide a solution to the digital divide which is quickly developing between units based on the shore with direct access to the GIG and remote units that must rely on satellite communications.

B. OBJECTIVES

The primary objective of this research is to demonstrate the efficacy of wireless networks based on IEEE 802.16 standards in supporting intra-battle group (Intra BG) communications in maritime, littoral and amphibious environments. This research builds on previous research conducted at Naval Postgraduate School in the employment of IEEE 802.16 wireless local area networks (LAN) in tactical environments, applications for use in current and future battle fields, and general vulnerabilities of the IEEE 802.16 protocol. This research investigates the use of two commercially available models of IEEE 802.16 wireless radios (Redline AN-80i and Motorola PTP series) for incorporation in an Intra-BG tactical network whose purpose is to facilitate the interconnection of individual IT-21 networks, voice over internet protocol (VOIP), video teleconferencing (VTC), tactical databases, and other existing and proposed NCW oriented information systems.

C. RESEARCH QUESTIONS

The research conducted during this study will focus on answering the following questions:

1. Is IEEE 802.16 wireless communications a viable solution for data communications in tactical maritime and littoral environments?

2. Can IEEE 802.16 networks be used to extend existing ship-based program of record (POR) accredited networks in use by the United States Navy?

3. Given two primary development paths for IEEE 802.16 wireless networks (single path or Multiple In, Multiple Out [MIMO]) which path will provide better link characteristics in a maritime environment?

4. What performance characteristics can be expected from IEEE 802.16 wireless LANs in a maritime environment?

D. SCOPE

The scope of thesis will include:

1. An analysis of key current and future communications needs of the United States Navy and Marine Corps.

2. An analysis of key network communications capabilities which are contained within a typical, deployed battle group.

3. Field experiments to test the performance characteristics of IEEE 802.16 wireless radios in maritime, littoral, and shore environments.

4. An analysis of deficiencies in IEEE 802.16 wireless radios which are currently available through commercial avenues, recommendations to correct those deficiencies prior to employment in tactical situations, and recommended areas to further study to support a tactical network based on IEEE 802.16 compliant wireless networking components.

E. METHODOLOGY

Research in support of this thesis will be conducted in accordance with the following methodology:

1. Detailed research into current network centric communications programs and their resulting requirements for data bandwidth.

2. Research into current military data communication assets and their associated unclassified performance characteristics.

3. Research previous thesis work conducted at Naval Postgraduate School in the areas of systems integration, performance measurement, network management, and vulnerabilities studies as they pertain to IEEE 802.16 wireless communications in different environments.

4. Market research into commercially available IEEE 802.16 wireless network solutions and current employment of the technology using commercial implementations as “market comparable” solutions to tactical military environments.

5. Perform phased laboratory and field experiments validating results obtained from previous research and in support of development of an IEEE 802.16 wireless tactical network to be deployed and operated in support of military field exercises.

F. ORGANIZATION OF THESIS

CHAPTER I: This chapter discusses some of the key issues facing military commanders and communicators as they pertain to digital communications in a NCW environment. The chapter also addresses the research purpose, methodology used during the research, and a framework for the thesis.

CHAPTER II: This chapter addresses the concept of Network Centric Warfare (NCW) and addresses the challenges faced by Commanders in a NCW environment as they pertain to the actual networking of disparate systems into a tactical network. It addresses current key communications efforts in progress by the Department of Defense to increase interoperability of tactical systems. Additionally, this chapter will look at current data networking capabilities of a typical battle group and analyze whether those capabilities are sufficient for future needs.

CHAPTER III: This chapter will discuss proposed characteristics of a tactical network, the efficacy of IEEE 802.16 based communication components in meeting those characteristics, and a proposed topology for tactical networks based on IEEE 802.16 protocols.

CHAPTER IV: This chapter will discuss the experimentation efforts conducted in support of this thesis and present the results of those experiments and conclusions drawn from them.

CHAPTER V: This chapter will present deficiencies found in the IEEE 802.16 protocol and commercially available IEEE 802.16 WLAN radios that were found during field experimentation and will present suggested solutions to those deficiencies. This chapter will also address areas that are suggested for further research in support of IEEE 802.16 WLAN employment in tactical maritime environments.

CHAPTER VI: This chapter presents a summary of the research and concluding remarks.

THIS PAGE INTENTIONALLY LEFT BLANK

II. NETWORK CENTRIC WARFARE COMMUNICATION CHALLENGES

A. OVERVIEW

Network Centric Warfare (NCW) is the current embodiment of the Department of Defenses' effort to harness the power of information technology to share information among geographically dispersed forces enabling commanders on all levels to request and obtain critical information regarding their battlespace space in order to more effectively employ their forces through achieving information superiority (Alberts et al. 7). Simply put the NCW concept calls for everyone to have immediate access to information contained on a multitude of platforms and have the ability to communicate with any one at any time for the purpose of planning and executing military operations.

What must be understood about NCW is that it is a conceptual framework of how information should be shared among war fighters on every level (Alberts et al. 6). It is not an architecture for building information systems or communications systems. Aside from calling for information and sensor systems to have the ability to seamlessly communicate with each other, NCW offers no concrete technological approach to achieving the goal of a "network centric" battlespace.

As NCW is only a conceptual view of information sharing and not a technical guide to implementation, the number of overall architectures for a NCW environment is varied. Additionally, NCW serves as an overall concept of operations for all of the military services enabling service-specific visions of NCW to develop. The Department of the Navy's vision of NCW is embodied in the FORCEnet concept. As defined in a joint statement by former Chief of Naval Operations Admiral Vern Clark and former Commandant of the Marine Corps Michael Hagee, FORCEnet is "the operation construct and architectural framework for naval warfare in the Information Age, integrating warriors, sensors, command and control, platforms and weapons into a networked, distributed combat force."

B. ENVISIONED ARCHITECTURE

Several efforts have been made to develop an overall architecture of a NCW based battle space, with little success. The most notable of the efforts is the Joint Technical Architecture published by the Joint Technical Architecture Development Group (JTADG) [JTA]. However, the title of the publication is deceptive. The JTA does not present an overall architecture for DoD components to follow while developing components and systems to integrate into an overall NCW architecture. The JTA presents two volumes of standards that the JTADG states should be followed by acquisition and development agents. The standards represent a compilation of commercial and military standards that all military information systems must use and be compatible with in order to be qualified as "joint capable". While falling short of a true architecture, the standards presented in the JTA do provide a "list of materials" for the services to use during the construction of new systems and revisions to existing systems. This "list of materials" can be thought of as the materials required for construction of a building. While the materials that are available to build the building are known, how to construct the building is unknown; there are no blueprints.

While the different services may have a different architectural rendering of an NCW environment, all of the architectures do share a common architectural use of satellite communications, land-based terrestrial communications (specifically GIG BE), and tactical wireless communication systems as illustrated in Figure 2. While this figure was extracted from a FORCEnet briefing, the same general overall architecture is seen in documents for Army, Air Force and Marine Corps NCW programs. One thing is certain for all of the initiatives, the amount of information that will be required to be transferred from unit to unit in a NCW environment will be exponentially greater that what is required today.

Several keys standards are mentioned in the JTA that have significant impact on current and future information system designs. The first key standard is for the use of TCP versions IPv4 and IPv6 (JTA). These are the primary protocols used in the majority of networks around the world. These protocols are also critical for any information system to be able to use the GIG as a means for transmitting data. Implied by the use of TCP IPv4 and IPv6 is the reliance on routable networks for information systems in a NCW environment.

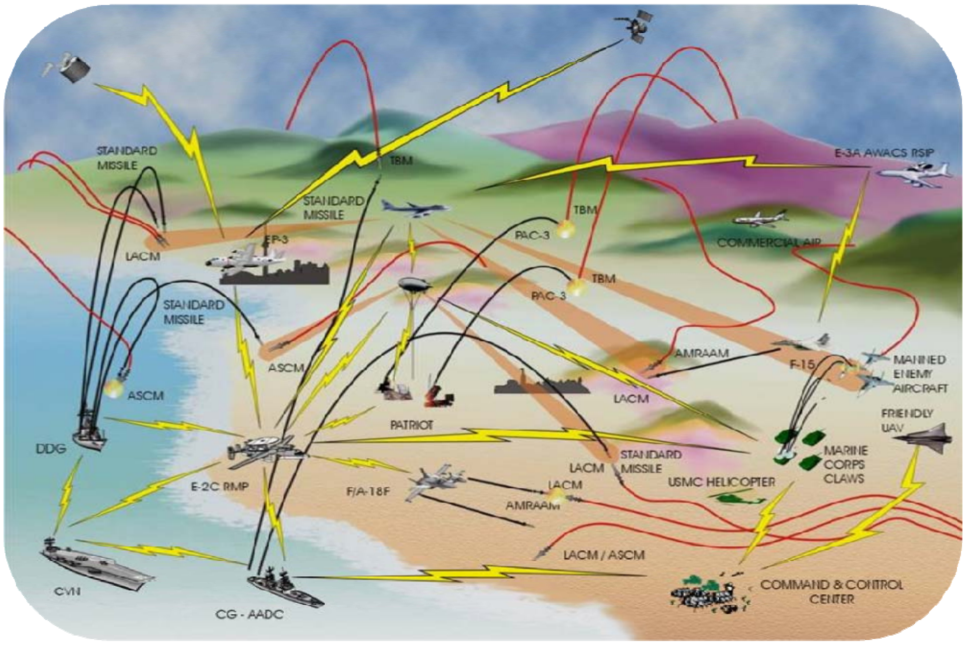


Figure 2 Notional Illustration of NCW Environment (From: Rodriquez).

Thanks to the completion of the Global Information Grid (GIG) Bandwidth Expansion (BE) program, a global high speed terrestrial network exists allowing military units access to networked assets on the GIG from any point in the world. When added to the constellation of military satellites operated by the DoD and commercially leased satellite assets, the GIG can be extended to any point on the globe be it on land or at sea.

The GIG, despite its capabilities, only provides the internetworking backbone for a NCW environment. In order to actually connect individual mobile units to the GIG, the concept of Mobile Ad Hoc Networks (MANET) must be employed. A MANET, in general terms, is a self-configuring area network comprised of individual unit networks connected to each other by wireless means creating a topology that is dynamic (Buddenberg 2). The key concept that must be derived from this definition is that the MANET must be architecturally driven, not application driven (Buddenberg 3). An example of this is shown in Figure 3. In this MANET architecture all of the units are connected to each other by a dynamic network created by a radio wide area network (radio-WAN). The important concept of this example MANET architecture is that it is completely application independent and scalable.

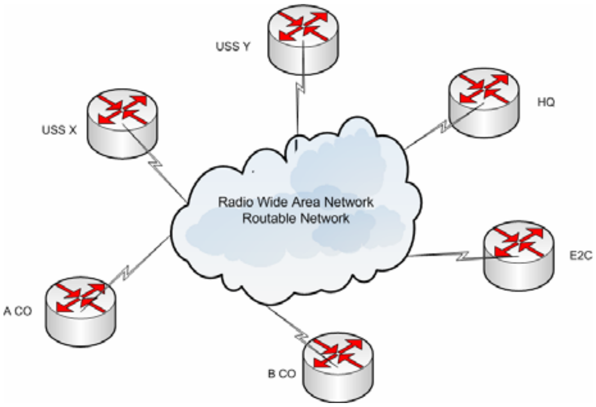


Figure 3 Basic MANET Architecture.

The MANET architecture shows multiple routed systems connected to a dynamic radio-WAN. At this point the architecture of the units must be considered. In the case of the example radio-WAN, a unit connected to the radio-WAN would consist of a routable network with multiple information systems and sensors connected to each other using the network as a Layer 1 medium. Many information systems on board U.S. Naval vessels are already connected using a network topology similar to this. When integrated with the concept of MANET architecture, all of the systems connected to the network of one unit can route data traffic to any of the other systems of another unit.

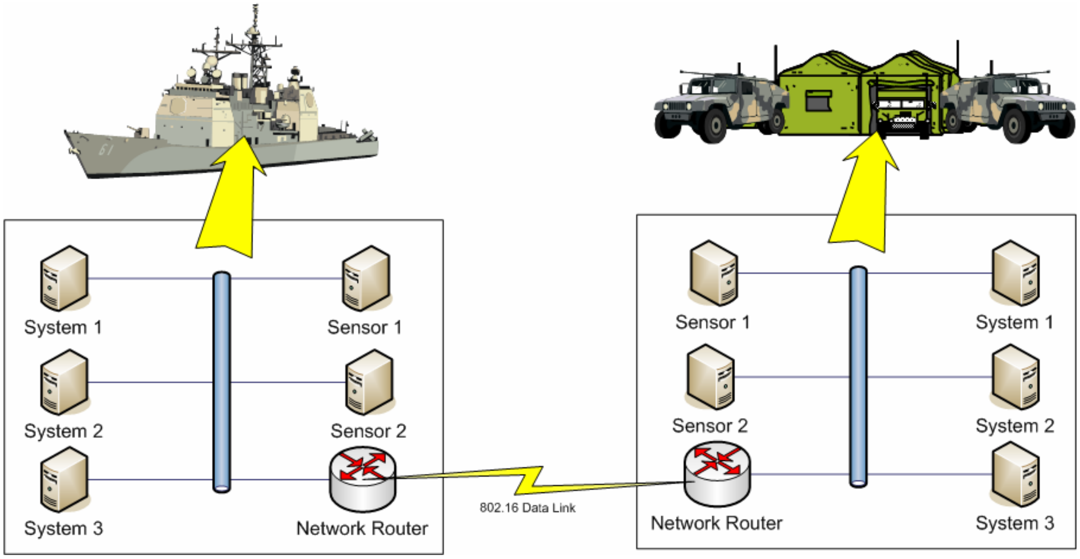


Figure 4 Example Routable Networks.

C. SYSTEM INITIATIVES

Many system development efforts have been undertaken since the origination of the NCW concept. As the services have begun to crystallize requirements, develop new information systems and upgrade existing information systems in order to be part of a joint communications and information architecture, the number of individual development efforts have skyrocketed. The following discussions are only a small sample of programs of record and systems under development. While not a complete listing of systems, they do serve to illustrate some of the current and future data needs of the U.S. Navy and Marine Corps.

1. Cooperative Engagement Capability

One of the best known information system development efforts is the Navy's Cooperative Engagement Capability (CEC) program. The purpose of this system is to seamlessly integrate sensors and weaponry from multiple platforms into a single common operational picture from which the Commander in the field can make informed decisions and more efficiently employee their assets. By combining the sensor and weapons capabilities of multiple platforms CEC extends the range at which ships in a battle group can detect and engage threats to beyond the radar horizon of any single ship (VPP 130)[2].

Most of the development effort behind this program appears to have been focused on the applications that will allow the sensors and weapons to be connected, not the physical means of connecting them. At this time, it is assumed that the primary means of transporting data between the platforms that comprise a CEC net will be a combination of satellite communications and TADIL J (Link 16).

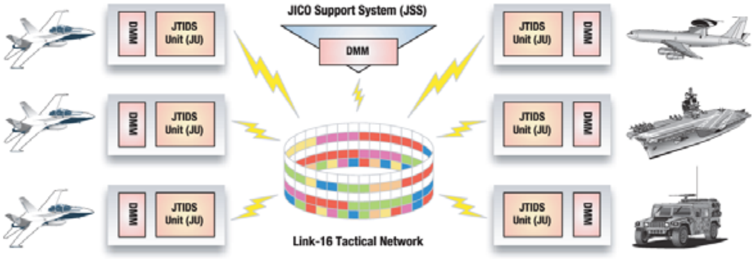


Figure 5 Example Link 16 Network (From: VPP).

a. Architecture

The overall architecture of the systems is envisioned to be a system of nodes (military units and sensors) interconnected to each other by a common system driven network (VPP 140). Each node will consist of a systems integrator which will combine all of the sensor inputs of the unit into a single operational database for that unit. This systems database will be connected to all of the other units in the CEC net by some means of data transport. When connected, the database of one unit will synchronize with the databases of all of the other units, combining their sensor pictures into a single common picture shared by all participants in the net which is continuously updated from the units own sensors and through continuous synchronization with the databases of all of the other units in the net. The end objective of CEC is not only provide a near-realtime common operational picture, but also to use that timely information to provide "fire control quality" information so that units participating in the CEC net can use the information displayed to identify targets, develop fire control solutions, and launch

[2] United States, "Vision Presence Power".

weapons against those targets (VPP 140). If successful, the system will effectively decouple weapons and sensors allowing for any one unit to use the sensors of any other unit to supply their weapons with accurate and timely data for military operations. Conceptually, the CEC network is no different than a conventional routable network based on IP protocols shown in Figure 6. However, as the system is not based on TCP/IP standards, it is not routable on traditional data networks.

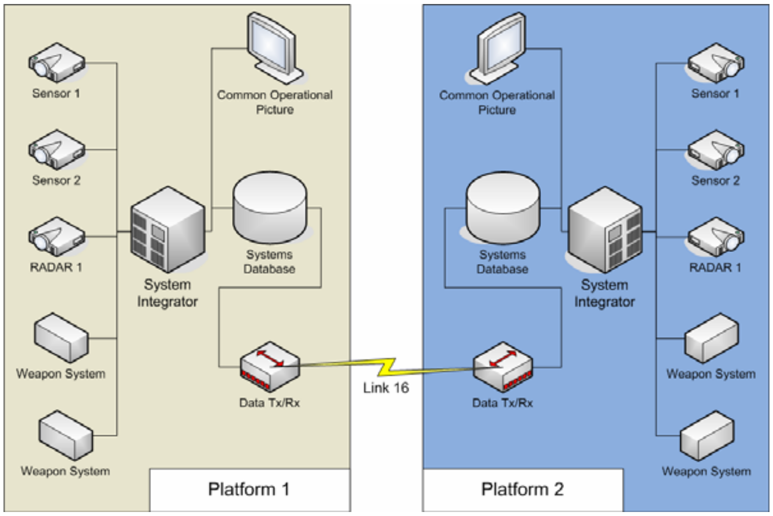


Figure 6 CEC Conceptual Diagram.

b. CEC Data Synchronization

As previously mentioned, each unit in a CEC net will have systems integration module which integrates and stores sensor and weapons information specific to that unit. Additionally, that database will be used to continuously synchronize information from all of the other units. The data storage requirement for a single unit is envisioned to be on the order of tens of gigabytes. When synchronized with other units, the size of the database will quickly explode to sizes on the order of hundreds of gigabytes. In order for the information to be “fire control quality” these databases must be continuously synchronized requiring a high bandwidth data network. According to the Congressional Research Service, program managers for CEC have expressed significant concern that existing and currently proposed data transfer mediums will be insufficient to handle the data transfer needs of a fully implemented CEC system (O’Rouke).

2. Distributed Common Ground/Surface System – Navy

Previously known as the Joint Fires Network (JFN), the Distributed Common Ground/Surface System – Navy (DCGS-N) is another effort to link disparate platforms together in a network centric environment in order to create a common operational picture developed and shared among those participating in the network (VPP 140). Instead of concentrating on weapons and sensors, DCGS-N concentrates on rapid dissemination of intelligence and imagery to members of the network allowing unit commanders a more complete picture of the battlespace. The program is joint effort to combine the ISR and information system capabilities of the Global Command and Control System – Maritime (GCCS-M), Joint Service Imagery Processing System – Navy (JSIPS-N), and Tactical Exploitation System – Navy (TES-N). The system uses the GIG to transfer information among the participants. Units can manually pull information from a DGCS-N central database or they can have information automatically forwarded to them based on mission requirements. Three levels of customers are defined for the system: Tier 1 – Numbered fleet command ships and ashore command centers, Tier 2 – Carrier and Expeditionary Strike Groups (CSG/ESG), Tier 3 – Unit level strike platforms (VPP 140).

The system component that immediately draws attention to DGCS-N is imagery. High quality and resolution imagery files can measure tens of megabytes each. When attempting to obtain a complete picture of the battlespace, hundreds of images can be required thus resulting in a requirement to transfer hundreds of megabytes of files between units on a frequent, if not continual basis.

3. Global Command and Control System Version 3.x

The Global Command and Control System (GCCS) is the end product of an effort to combine the capabilities of multiple earlier command and control systems into a single architecture capable of displaying a common operational picture (ICMC 2-19)[3]. First introduced in the mid-1990s, GCCS represented a major leap forward in battlespace management and information management. Since introduction, GCCS has become a

[3] United States, Information and Communication Managers Course (CIN: A-202-0041C).

product-line architecture with variants for maritime, air, land and joint operations. This system has also become a critical tool for operation planning and execution. While originally designed to transfer data between GCCS systems using the Officer in Tactical Control Information Exchange System (OTCIXS), GCCS is now capable of synchronizing GCCS systems through IP connections to a data fusion center located at shore sites around the world (ICMC 2-19). It is now not unusual for a GCCS system to be able to display 6,000 tracks in near-real time.

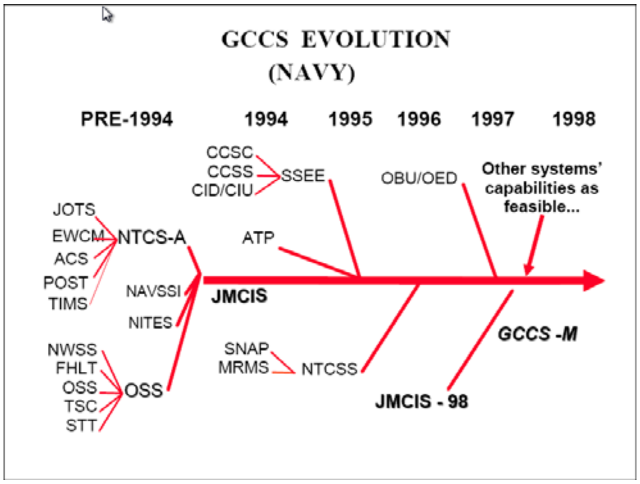


Figure 7 GCCS Evolution (From: ICMC).

4. Global Command and Control System 4.x

With the success and wide acceptance of GCCS 3.x, a development effort was launched to update GCCS 3.x to allow it to become “the” command and control system for use by all branches of the United States military. The design of GCCS 4.x, also referred to as GCCS-J, eliminates the systems reliance on specialized hardware and software (ICMC 2-20). The design also calls for the integration of more detailed information for each entity the system tracks such as associated imagery, links to relevant information about the track stored on other sources, etc. This addition of data represents a potential critical tool for GCCS users, however, it also represents an explosion in the amount of data that GCCS must store, process, and transfer to and from other units. While databases in GCCS 3.x systems are measured in hundreds of megabytes, the databases in GCCS 4.x systems will most likely be measured in hundreds of gigabytes. At the time of this thesis, the fielding date for GCCS 4.x is unknown.

5. Combined Enterprise Regional Information Exchange System

The Combined Enterprise Regional Information Exchange System (CENTRIXS) has become a critical tool for classified communications with coalition partners around the world. Due to security restrictions and issues of releasibility, variants of CENTRIXS have been developed and deployed to forces in different regions that have different coalition partners. Variants of the system include (VPP 138):

- CENTRIXS Four eyes (AUS/CAN/UK/U.S.)
- CENTRIXS Japan (J)
- CENTRIXS Korea (K)
- NATO Initial Data Transfer System (NIDTS)
- Global Counter Terrorism Task Force (GCTF)
- Combined Naval Forces CENTCOM (CNFC)
- Multi Coalition Forces Iraq (MCFI)
- Cooperative Maritime Forces Pacific (CMFP)

CENTRIXS enables ship-to-ship and ship-to-shore networking enabling members of the network to share information using a web-based environment (VPP 139). Each component of the network has a web server which acts the portal to the network. Unlike typical web-based systems where users connect to a distant server to access information, the CENTRIXS system continuously synchronizes all of the servers on the network allowing units to connect to the local server and access the same information available to all other participants even when the data links supporting the network go down. Depending on the nature of the operation, the size of the web contents can range from dozens of megabytes to gigabytes.

CENTRIXS is not an independent network. The system uses VPN technology to create a virtual network for use by the system; in all cases CENTRIXS uses SIPRNET to "host" this virtual network (VPP 139). Hence any bandwidth considerations for SIPRNET must also include CENTRIXS.

6. Video Teleconferencing

Video teleconferencing (VTC) has become a critical tool for commanders to use to collaborate with multiple organizations during mission planning and actual operations. While allowing commanders to collaborate with sites thousands of miles apart, VTC transmissions also represent a significant drain on the available bandwidth for military units. A medium quality VTC will require 128 kbps of SATCOM bandwidth (ICMC 4-15). For ships with limited bandwidth to begin with, VTCs typically force bandwidth reduction for other systems, or the shut down of those systems, for the duration of the VTC.

7. Plain Old Telephone System (POTS)

All large naval vessels will have "at sea" circuit switched telephone lines associated with their unit to maintain telephone communications with the shore while at sea. In the case of numbered fleet command vessels, as many at 15 at-sea telephone lines can be associated with the ship. In order to maintain these telephone lines, bandwidth must be allocated at all times for their support. In most cases each POTS[4] line is allocated 64 kbps. In some cases the bandwidth can be reduced to 32 kbps; this also results in lower fidelity phone calls. In the case listed above, for 15 at-sea lines operating at 64 kbps per line 960 kbps of dedicated bandwidth is required on a continual basis; bandwidth that is not available for use by any other system.

8. Voice over Internet Protocol

Voice over Internet Protocol (VoIP) is quickly becoming popular in the military. Capable of transmitting telephone calls over standard IP data links with little specialized

[4] POTS – Plain Old Telephone System. Circuit switched telephone system.

equipment required, VoIP is now in wide use through out theaters of operation. As part of the overall GIG BE program Defense Switched Network (DSN) POTS circuits are being replaced with a VoIP packet switched telephone system (DISA).

As with POTS lines, each VoIP call requires a certain amount of bandwidth. High quality phone calls require 64 kbps; medium qualities require 32 kbps. However, unlike POTS lines, VOIP lines do not require a dedicated allocation of bandwidth. When a VOIP call is initiated, it uses the bandwidth of the network that it “rides” on (i.e., NIPRNET, SIPRNET, etc.) When the call is completed, the bandwidth is returned for use by the network.

9. Summary

The systems discussed in this section do not, by any means, represent an all inclusive list of systems and applications in operation in the United States Navy and Marines Corps. The systems discussed only serve as a small sample to illustrate the current data needs of the United States Navy and Marine Corps and also show that the data needs will only increase in the future

D. SATELLITE COMMUNICATIONS OVERVIEW

1. Discussion Note

Due to the sensitive nature of military communications in general and satellite communications in particular, only publicly available characteristics of military satellite systems will be discussed in this section. Additionally, the sample communications plans used in this section do not represent actual communication plans. However, the values used give an adequate representation to illustrate the bandwidth allocation decisions that every Communications Officer in the military must face when dealing with satellite communications.

2. Background

Currently, the United States military operates the largest “privately” owned constellation of satellites in the world. Military satellites provide a critical means of communication to every unit afloat and ashore and the primary means for extending the GIG to those units. Without the military SATCOM system, the military's operational efficiency would drop dramatically. Without military SATCOM, NCW will be impossible.

Prior to beginning a discussion about SATCOM, a key concept must be presented. Satellite bandwidth allocations for ships and ground units are controlled by the area's unified commander. The J6 of the Combatant Commander (COCOM) staff will allocate bandwidth among the services operating the area. That bandwidth is then subdivided by the senior service commanders in the area to their subordinate units (ICMC 12-2). Thus, if a satellite system is shown to be capable of a total downlink bandwidth of 100 Mbps, it must be understood that bandwidth is divided among all of the operational units serviced by that satellite. For example, assuming there are 100 units being serviced by the satellite and each unit receives an equal allocation of bandwidth, each unit will only be authorized to use 1 Mbps of the total bandwidth.

The previous section discussed some of the current and future data needs of the United States Navy and Marine Corps. As can be seen, the amount of data that must be transferred already is a tremendous amount. As Network Centric Warfare (NCW) becomes a larger part of military operations, both doctrinally and operationally, the amount of data that must be continuously transferred to large and small units in both unicast and multicast transmissions will increase beyond our current SATCOM and terrestrial LOS capabilities.

3. Defense Satellite Communications System

The Defense Satellite Communication System (DSCS) is a set of geostationary SHF communications satellites operated by the Defense Information Systems Agency (DISA). The constellation of DSCS satellites is comprised of nine SHF wideband satellites which provide unicast IP data links to military units around the world; on land and at sea. This system is also the primary entry point to the GIG for all mobile military units (ICMC 7-19).

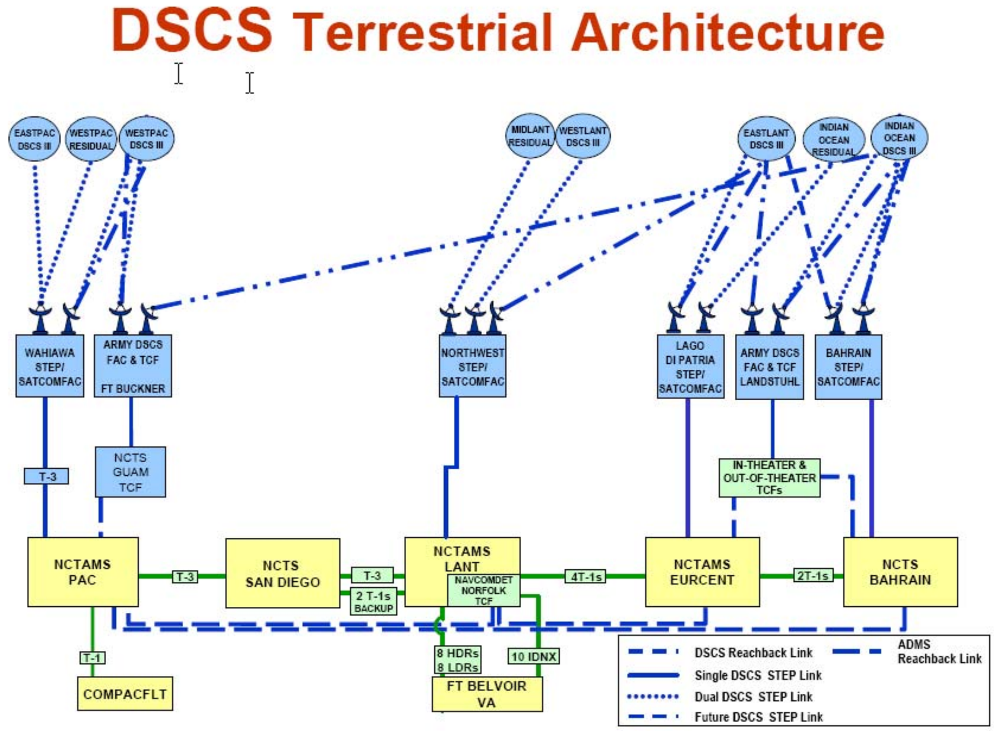


Figure 8 DSCS Terrestrial Architecture (From: ICMC 7-19)

4. Navy Ultra High Frequency Follow On Satellite Program

The Navy's Ultra High Frequency (UHF) Follow On (FO), also known as UFO, satellite program was launched in the 1990s as a replacement for the Fleet Satellite Communications (FLTSATCOM) constellation of satellites. The UFO constellation provides secure data and voice communications for ships, ground forces, and airborne platforms around the world. Throughput to ground terminals varies depending on the platform. As the system operates with a narrow bandwidth, throughputs are limited to 64 kbps and below per channel. While this is a very small throughput when compared to other systems, it is a vital means of communications to mobile ground forces using small ground terminals. The UFO constellation is already scheduled for replacement by the Mobile User Objective System (MUOS) beginning in FY 2008 (ICMC 6-4).

5. MILSTAR

The MILSTAR satellite constellation was developed and deployed in the 1980s and 1990s to facilitate strategic non-IP based communications to strategic commands around the world. Since strategic tensions have eased with Russia, the original purpose of the constellation has become secondary (ICMC 9-4).

The MILSTAR system is now a joint service satellite communications system that provides secure, jam resistant, worldwide communications to meet essential wartime requirements for high priority military users. The multi-satellite constellation links command authorities with a wide variety of resources, including ships, submarines, aircraft and ground stations.

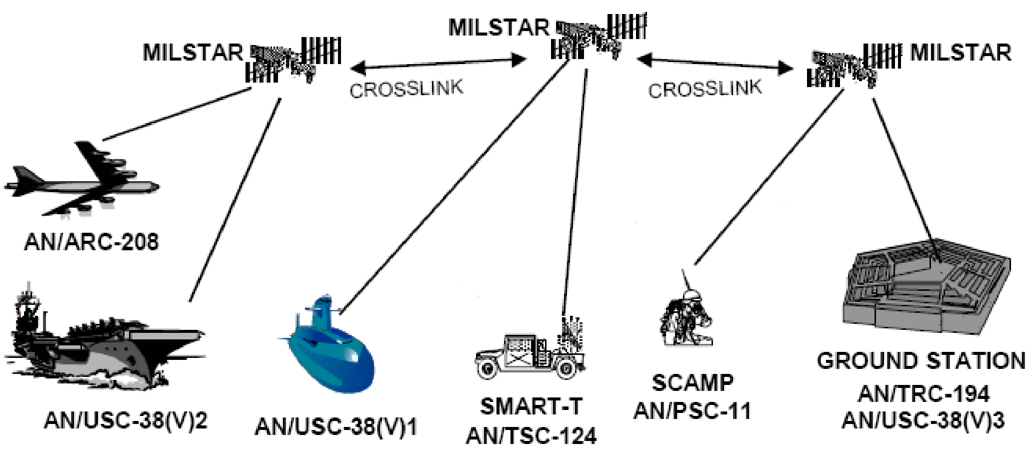


Figure 9 EHF SATCOM Notional Architecture (From: ICMC 9-5).

The operational MILSTAR satellite constellation consists of five satellites positioned around the Earth in geosynchronous orbits. Each MILSTAR satellite serves as a router by directing traffic from terminal to terminal anywhere on the Earth. Since the satellite actually processes the communications signal and can link with other MILSTAR satellites through cross-link channels, the requirement for ground controlled routing is significantly reduced.

Two variants of ground stations exist which provide data rates of 9600 bps (Low Data Rate) up to 1.544 Mbps for Medium Date Rate (MDR) variants. While this data link is available on most large ships, it is typically reserved for high importance tactical and strategic communications.

6. INMARSAT

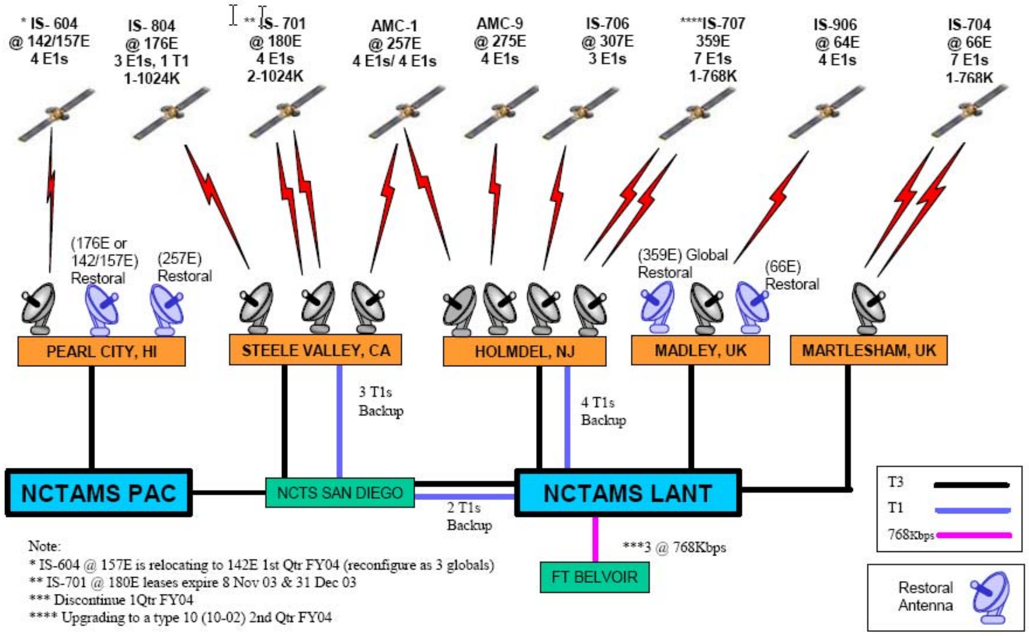
The International Maritime Satellite (INMARSAT) communications system is a commercially operated constellation of communications satellites which provide low bandwidth, global communications for both civilian and military users. Most INMARSAT terminals are single channel terminals operating at 64 kbps (ICMC 6-32). Dual channel terminals are capable of up to 128 kbps. Recent improvement to U.S. Navy INMARSAT terminals allow for bandwidths up to 196 kbps. Large ships do not rely on INMARSAT for their primary satellite communications, however, small ships such as Perry class frigates do rely it for their primary means of SATCOM.

It must also be noted that INMARSAT channels are not owned by the Navy or the Department of Defense; they are leased. Typical monthly leases per channel are approximately $20,000 (ICMC 6-33).

7. Commercial Wideband Satellite Program (CWSP)

The CWSP was initiated in 1992 in response to the Navy's growing need for satellite communications and the slow pace of funding, development, and deployment military satellite systems. The program is based on a commercial-off-the-shelf (COTS) model which uses military ground terminals to connect to commercially owned satellites and military owned ground stations (ICMC 7-21). Using this arrangement, the Navy leases the excess bandwidth available on the commercial satellites for military communications. However, if that excess bandwidth is needed by the commercial operator, it can be taken away from the Navy[5]. Figure 10 shows the general architecture of the CWSP system.

[5] This situation occurred during the 2000 Summer Olympics in Sydney, Australia. The commercial satellite operator of the satellite servicing the Pacific AOR needed additional bandwidth for press coverage of the Olympics. Navy bandwidth for CWSP was reduced for the duration of the Olympics.



Note:
* IS-604 @ 157E is relocating to 142E 1st Qtr FY04 (reconfigure as 3 globals)
** IS-701 @ 180E leases expire 8 Nov 03 & 31 Dec 03
*** Discontinue 1Qtr FY04
**** Upgrading to a type 10 (10-02) 2nd Qtr FY04

Figure 10 CWSP Architecture (From: ICMC 7-22).

8. Global Broadcast System (GBS)

The Global Broadcast System (GBS) is not an independent satellite system. The system exists as payloads on the UFO-8, 9, and 10 satellites of the UFO constellation (VPP 182). The system provides non-contiguous global coverage, shown in Figure 11. This satellite system provides high bandwidth, simplex service to units with GBS receiving stations. Each unit acts as a subscriber and orders services and products from the GBS uplink stations. Those services are then loaded into the GBS network databases at injection points across the globe and automatically downloaded by the receiver station terminals. The service acts as a supplement to other SATCOM by providing high volumes of data and streaming video at rates up to 30 Mbps (VPP 182). Since the service is simplex, no uplinks can be made using GBS.

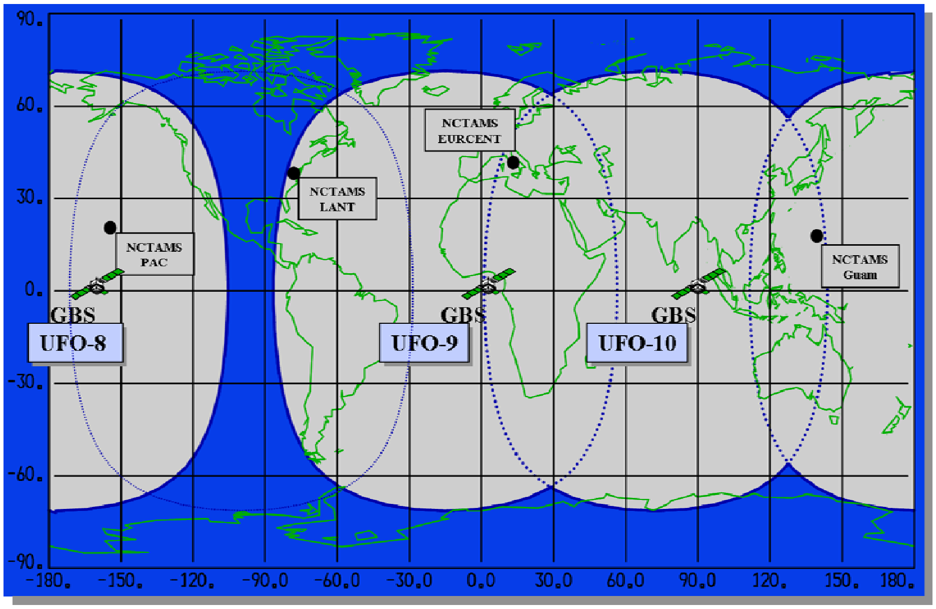


Figure 11 GBS Coverage Map (From: ICMC 7-26).

9. Tactical Data Information Link - J

The Tactical Data Information Link - J (TADIL J), also referred to as Link 16, is a UHF data communications system whose purpose is to provide Navy ships, tactical air and Marine Corps ground units with secure, jam resistant, low bandwidth tactical communications (VPP 134). Units equipped with TADIL J are capable of providing integrated communications, navigation and IFF capabilities among those units participating in the TADIL J net. The system is interoperable among all services and NATO/Allied users equipped with TADIL J communications equipment, however, it is not designed to be part of a routable IP-based network.

Communications with TADIL J can also be carried over UHF SATCOM allowing for beyond the horizon communications with other participants equipped with TADIL J SATCOM capabilities. However, TADIL J throughput over UHF SATCOM is very low and measured in baud (VPP 135).

It must be noted that the datagrams carried by the TADIL J system are system specific and capable of being used only by TADIL J equipment; it is not capable of carrying IP traffic. This system is mentioned in this section because of its SATCOM capability.

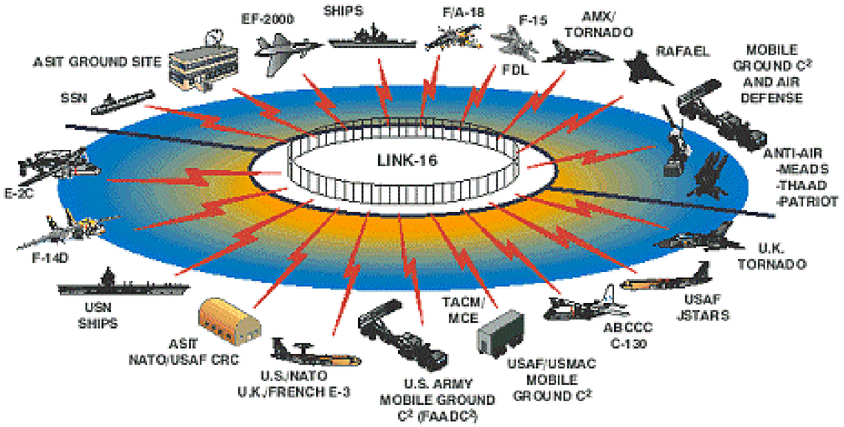


Figure 12 Conceptual TADIL J Net Architecture (From: VPP 150).

E. TERRESTRIAL RADIO COMMUNICATIONS OVERVIEW

While SATCOM is a vital part of military communications, terrestrial radio communications bring the network down to the field unit level. This discussion will only cover five terrestrial systems capable of IP data communications. This is not an all inclusive listing of data capable military radios. However, for the sake of brevity, only the most advanced systems were chosen for this discussion.

1. Digital Wideband Transmission System

The function of the Digital Wideband Transmission System (DWTS) is to provide secure, bulk encrypted voice and data ship-to-ship and ship-to-shore communication links for littoral and amphibious warfare units. The system was developed as a replacement for the AN/VCC-2 VHF multi-channel radio series and provides a data path to the GIG when connected to shipboard ISNS network systems on U.S. Navy ships (DWTS)[6].

[6] United States: Department of Defense. COTS Equipment for The navy shipboard UHF Digital Wideband Transmission System (DWTS).

DWTS was designed to operate close in (approximately 10 nm) to the shore in LOS conditions with the receiving unit. The system was designed to operate only in a point to point architecture at date rates ranging from 256 to 2048 kbps (DWTS).

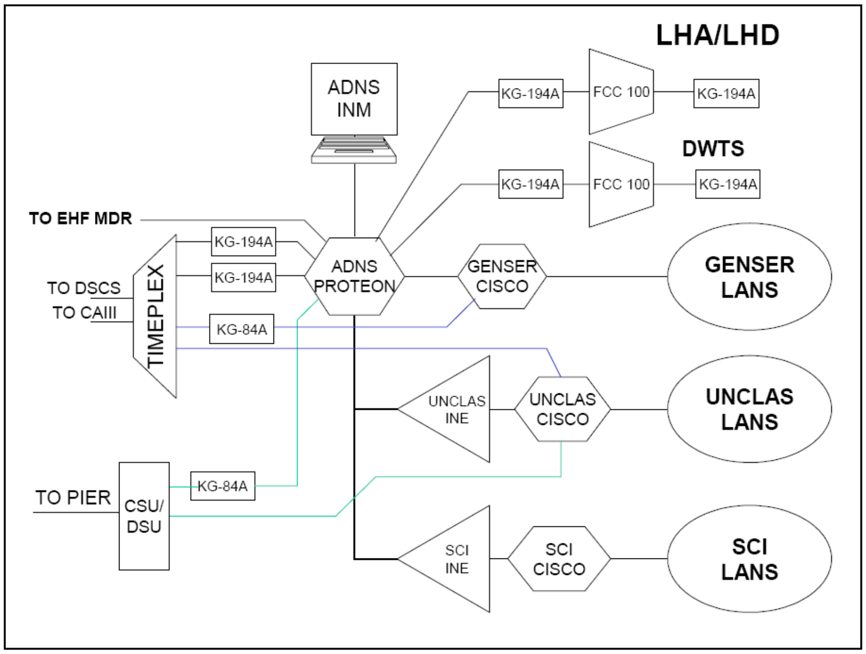


Figure 13 Basic LHA/LHD Shipboard Network Topology (From: ICMC 7-20).

2. Enhanced Position Location Reporting System (EPLRS)

The EPLRS radio is a handheld UHF radio which provides secure UHF networked digital data radio providing on-the-move medium rate communications to DACT-equipped[7] combat units down to the company level. The ELPRS radio was not specifically designed for IP data communications; it was designed for position location of units equipped with the system. However, it has been modified to allow data rates on the order of 32 kbps in LOS conditions to ranges of 10 nm (Bey).

[7] Data Automated Communications Terminals (DACT) - provides a handheld end user terminal for vehicular or dismounted ground forces to display battlefield maps overlaid by near real-time friendly and suspected enemy location information. DACT has Global Positioning System (GPS), digital maps, and moving map display.

3. Joint Tactical Radio System (JTRS)

The JTRS program is an on going program designed to produce secure voice and data links between multiple military radios on multiple platforms. The radio system is envisioned to be software programmable and capable of operating over multiple military and commercial frequencies, eliminating the need for field units to carry multiple radio systems for different communication needs (North et al. 3-1). While an exceptional idea, the JTRS program has faced a multitude of program setbacks and cost overruns. The date for operational fielding of JTRS is unknown.

4. Secure Digital Network Radio (SDNR)

The SDNR, also known as the VRC-99 radio, is a digital capable radio which operates in the VHF frequency range providing data throughput of up to 625 kbps. The VRC-99 was originally developed for the Army and later adopted by the USMC. In recent experiments, VRC-99 radios have been placed on naval surface platforms and E-2C Hawkeye ISR platforms enabling limited data communication between airborne and surface units. While functional for small units, VRC-99 nets are only capable of servicing up to 16 units at one time (Global Defense).

5. Global Information Grid (GIG) Bandwidth Expansion (BE)

The GIG BE program is a terrestrial IP based network providing high bandwidth networking to over 80 critical network operation stations around the world using commercial of the shelf (COTS) technology. The system provides the terrestrial network backbone for all of the Department of Defense with speeds up to OC-192 (10 Gbps) [DISA]. Due to its terrestrial nature, mobile units at sea or units in the field do not connect directly into the GIG. For these units, the only connection to the GIG is through SATCOM significantly limiting the bandwidth available to these units. The GIG is also application independent and architecturally driven. This means that if and when the some or all of the components of the GIG must be replaced, the applications using the GIG will feel no impact.

F. SATCOM USAGE

After reading the previous section, one might think that there is plenty of bandwidth on the military SATCOM systems and terrestrial systems to satisfy all of the military's bandwidth needs. Unfortunately that is not the case. Even with the high bandwidth available to military units using the GIG BE network backbone, the limiting factor for deployed military units is SATCOM.

During Operation Iraqi Freedom military SATCOM, as a whole, operated at 100% capacity. Military SATCOM systems could not provide enough bandwidth for units in the Persian Gulf and Iraq; more satellite bandwidth was needed. As a consequence, DoD contracted additional bandwidth from commercial sources. In the end, over 80% of all satellite communications used by the military during OIF was provided by commercial SATCOM systems (O'Rourke). This represents a 400% overload of military SATCOM systems. As NWC operations continue to increase and more NCW applications come on line, military SATCOM usage and reliance on SATCOM will only increase.

G. SATCOM BANDWIDTH PLANNING BASICS

An unfortunate reality that any communications officer must face is that just because your SATCOM system is capable of achieving a bandwidth of 2 Mbps does not mean that you will get all of that bandwidth. Bandwidth on military SATCOM systems is tightly controlled by necessity. Control over bandwidth is exercised by satellite ground control stations, Unified Commanders, and CTF Commanders. By the time a unit is allocated SATCOM bandwidth, they may only receive an allocation of 768 kbps for a system capable of 2 Mbps. This is one of the first realities of unit level bandwidth planning (ICMC 14-2).

The second reality of SATCOM bandwidth planning is that once a unit receives their bandwidth allocation communication officers must then sub-allocate that bandwidth to systems requiring access to the GIG. For this discussion it will be assumed that the maximum bandwidth has been allocated for an afloat unit using DSCS; 2048 kbps.

As an example let us assume that only four systems will require bandwidth: NIPRNET, SIPRNET, VTC, POTS Telephone circuits. Though physically separate systems, they will be combined into a single data stream using a multiplexer and then sent through the SATCOM system to a terrestrial station for further routing to their appropriate destinations. For this example let us assume that the systems have the following requirements:

System	Bandwidth Requirement (kbps)
NIPRNET	512
SIPRNET	768
POTS (10 lines at 64kbps per line)	640
VTC	128
Total	2048

As can be seen, the 2048 kbps that was allocated to the unit is now allocated for use by multiple systems. In the case of SIPRNET a large naval vessel (i.e., CVN, LHD, LCC), that 768 kbps could be share among 100 systems (workstations, servers, tactical systems, etc.) reducing the bandwidth per workstation to 76.8 kbps. As a point of comparison the maximum speed of a dial up modem is 56.6 kbps. If this example seems a bit extreme, what is the communications officer on board a United States Navy Oliver H Perry class Frigate (FFG) with a total SATCOM bandwidth of 196 kbps[8] going to do?

H. NETWORK CENTRIC WARFARE (REVISITED)

As the military continues to move to a NCW oriented doctrine and more joint systems are developed to enable commanders from the National Command Authority level down to the unit level to share the same common operational picture, the demands on military communications will overload our current capacity. If SATCOM remains the predominate means of data communication between units, how is a capacity-constrained FFG going to fully participate in the common operational picture with a maximum SATCOM throughput of 196 kbps? A soldier?

In an NCW environment, multiple data transmission systems must be combined to provide compatible inter-network data paths so that all units participating in an NCW

[8] Based on the assumption that the FFG is outfitted with INMARSAT B FC 6.

environment have access to the same information in a timely manner. Additionally, constructing a NCW network in a modular, common protocol-based architecture, vice a systems based architecture, will enable the networks to become decoupled from the systems which they support and. This will allow applications to become more flexible and allow the network which connects them to be replaced with new means of transport with little affect on the applications.

I. TACTICAL NETWORKS

Tactical networks are the enabling factor of an NCW organization. From a conceptual point of view, NCW architecture in an area of operation is organized in holonic[9] groups. The units that comprise each holon must share information between the units of that holon, other holons, and with organizations higher in the command structure. Using current means of data communications, bandwidth between the units of an individual holonic group is wholly limited by the limitation of SATCOM communication. The same is the case with communication between holonic groups. However, when a tactical network is implemented within a holonic group, communications are no longer limited by SATCOM; SATCOM is supplemented by the tactical network.

1. Example Scenario

If we take this architecture and apply it to two units operating in an area, we develop a communications structure shown in Figure 14. As can be seen, the two units are geographically located 10 nm apart and for this example communicate using military SATCOM at 768 kbps. In order to maintain a current and accurate COP they must continuously synchronize a 2 GB database (for this example we will also assume that they must transfer the entire database.)

[9] Coined by Arthur Koestler from the Greek 'holos' meaning whole, and 'on' meaning entity, as in proton or neutron; hence a holon is a whole to those parts beneath it in a hierarchy but a part to those wholes above it.

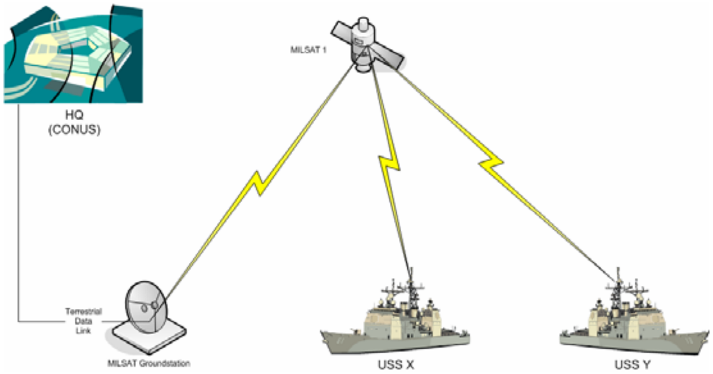


Figure 14 Example NCW Architecture.

a. Transfer Time

With a bandwidth of 768 kbps available to both units, it will take almost 45 minutes to completely transfer the 2 GB database. By the time the transfer is complete, the data is at least 45 minutes time-late and useless for most tactical purposes. Even if the synchronization only requires transferring 100 MB of data, it would still take 2 minutes to transfer the database making the data useless for any air warfare operations or missile defense. These times are unacceptable for a COP scenario.

b. Distance

The units in this example are geographically located 10 nm apart. In order for USS X to send a data message for USS Y using traditional DSCS SATCOM, USS X must send the message up to the MILSAT, which will relay it to the Ground Station, which will route it back up to the MILSAT, which will relay it to USS Y. The message that USS X sent to USS Y traveled over 88,000 miles and incurred a latency of over 1,500 ms in order to travel a lateral distance of 10 nm. This is an extremely inefficient means of communicating within a holonic group.

2. Proposed Solution

As seen in the example, intra-battle group (holonic group) communication using SATCOM is an extremely inefficient means of communication. A more efficient means of communications between the units is an intra-battle group tactical network. This tactical network would allow the units to establish a direct data communications link between them and eliminating the need to use SATCOM for direct communications between them as shown in Figure 15.

The tactical network does not eliminate the need for SATCOM, this must still be used for beyond the horizon communications and in the event that the tactical network is distrupted. However, the tactical network does significant reduce the need for SATCOM.

Admittedly, NCW does call for tactical networking with holonic groups. However, little visible development has been performed to develop tactical networks adequate to meet the communication needs of units in a NCW environment.

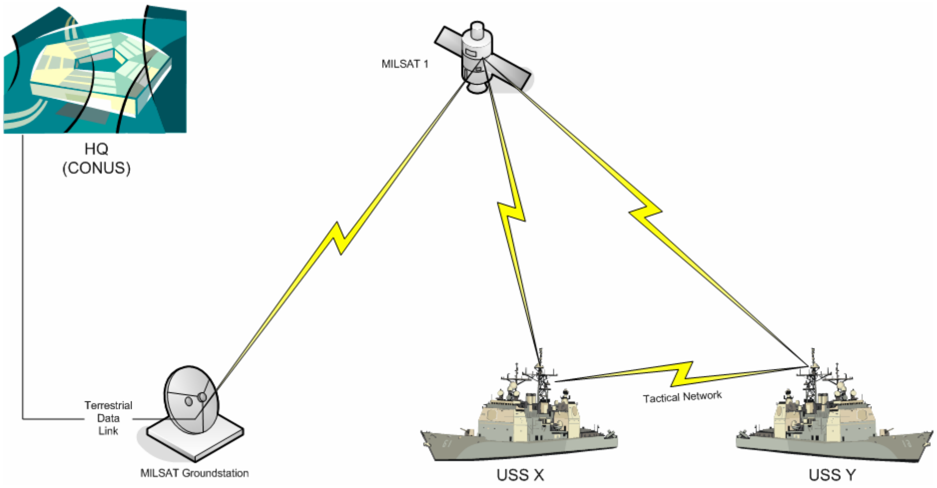


Figure 15 Basic NCW Architecture with Tactical Network.

There are two systems already in service that can serve as terrestrial data networks within holons: Link 16 and DWTS. However, they have the following failings:

- Link 16 –
    - Available throughputs using Link 16 are limited to 64 kbps;
    - Not all military units are Link 16 capable;

    - Not all coalition partners are Link 16 capable;
    - Datagrams on the Link 16 data link are non-IP based and non-routable.
- DWTS –
    - Throughput is limited to 2048 kbps (best case scenario);
    - Not all ships have DWTS (installation is limited to amphibious class ships);
    - DWTS is not a coalition system;
    - The system is point-to-point only.

These failings make both Link 16 and DWTS unsuitable for a primary means of communications, in most cases, for an intra-battle group tactical network.

A more appropriate means to establish an intra-battle group tactical network would be through the use of IEEE 802.16-based wireless radios. The use of such radios would enable a high bandwidth data link between the units of the battle group, create a routable wide area network based on architecture needs instead of being application driven, and reduce the need for SATCOM while enabling the tenets of the NCW concept. Additionally, the same conceptual tactical network architecture can be applied to units operating in littoral, amphibious, and shore-based environments. The remainder of this thesis will focus on the characteristics and capabilities of IEEE 802.16-based wireless radios in a tactical environment showing the efficacy of these systems in creating a NCW environment.

THIS PAGE INTENTIONALLY LEFT BLANK

III. TACTICAL NETWORK CHARACTERISTICS AND A PROPOSED IEEE 802.16 BASED ARCHITECTURE

As mentioned in the previous chapter, current and proposed military satellite communications (SATCOM) alone, as asserted by the author, will not fulfill the data transfer needs of a network centric battle force as conceptually or architecturally envisioned. Internetworking and interconnection of geographical dispersed information systems and networks cannot be performed by SATCOM alone. The interconnection must use a variety means in order to connect squad level, regiment level, battle group level and major commands into a single cohesive network allowing for all levels of command to share information not only between hierarchical levels, but also horizontally.

While future SATCOM promises to greatly increase the available SATCOM bandwidth to military units around the world, past history has shown that bandwidth requirements have outpaced available bandwidth by a significant amount. If this growth trend continues and the dogmatic approach to “SATCOM only” communications continues future military SATCOM systems will become obsolete before they are deployed. A potential solution is to decrease military reliance on SATCOM communications by shifting the burden of “local” tactical communications from SATCOM to a terrestrial tactical network communications system enabling tactical level communications while still providing a means for connecting local units to other units beyond the range of the tactical network.

Given this need for a tactical network, what are the characteristics and capabilities that it must have in order to satisfy the needs of the units that it services? This section will address that question as well as how a wireless tactical networks can supplement communication systems already in use by the U.S. and coalition militaries.

A. COMMERCIAL WIRELESS COMMUNICATIONS HISTORY

Since the first IEEE 802.11 wireless network devices came on the commercial market around 1995, wireless communications has experienced exponential growth and advancement. Consumers quickly discovered that they were no longer bound by the wired network world and could operate virtually anywhere while still connected to a network. Since the introduction of IEEE 802.11 compliant devices several other IEEE wireless standards have been developed to further expand the capabilities, mobility and security of wireless networking.

The IEEE 802.16 standard was first ratified in 2001 (IEEE 802.16-2001). The protocol acknowledged the short comings and security flaws of the IEEE 802.11 standard and sought to build a protocol which ensured high quality service and high levels of security in a wireless system. Since the original IEEE 802.16-2001 standard, the protocol has experience significant maturation and additional significant revisions in 2002, 2004, and 2005 incorporating mobile networking, mesh applications, and MIMO technology into the protocol (IEEE 802.16-2005). In its current iteration, IEEE 802.16 is poised and ready to enter the realm of military communications to provide high bandwidth wireless networking to users at sea and on land.

B. TACTICAL NETWORK CHARACTERISTICS

Tactical radio networks are dynamic and ad hoc by their very nature; tactical data networks will be no different. While military communication planners diligently attempt to design communication networks prior to military operations, rarely do the actual networks look like the designed networks. These variations are inevitable due to the amount of unknown variables that communication planners face such as the actual number of units that will participate in the network, the physical environment of the network (i.e., terrain, weather, propagation effects), etc. Due to this fact, planners must build the best core network that they can and plan for variations at the edges of the network; the unit level. With this in mind, the following characteristics are proposed for a tactical network supporting maritime operations and limited ground and amphibious operations:

1. High Quality of Service

This characteristic is one of the most important characteristics of any network; radio or data. Simply put, if a network cannot provide the services that are required of it in a timely manner the network is not worthy of service. However, this overall classification of "quality of service" can be divided into multiple characteristics that work together to give an overall quality of service. It must also be noted that of the sub-attributes of QoS listed below, that QoS as a whole is a trade-off between these characteristics as they may not all be achievable at the same time.

a. Bandwidth Efficiency

Bandwidth efficiency is the ability of a wireless data system to make the most efficient use of the frequency bandwidth the radio operates in. Inherent to this definition is the use of scheduled message deliver and system access methods using scheduling MACs. Contention based delivery means, such as Carrier Sense Multiple Access (CSMA), perform poorly with respect to bandwidth efficiency. Any system used for a tactical network needs to have a high bandwidth efficiency.

b. Network Determinism

This facet of QoS is the ability of the network to guarantee that a packet of data is transmitted and received in a finite amount of time. Without determinism in the network, there is no guarantee when the data packet will get to its destination (Buddenberg). Additionally, determinism is a key component of ensuring collision-free network operation further improving the efficiency of the network.

c. Low Latency

Latency refers to the amount of time it takes to transmit a message from one to when it is received at its destination. In the case of a tactical network, low latency is a critical requirement. With SATCOM a user can always expect latency on the order of 1500 ms (1.5 seconds)[10]. When attempting to develop a firing solution on a fast

[10] This latency estimation is an "order of magnitude" estimation based on the author's experience with military and commercial satellite communication systems. Due to distance of communication satellites from Earth, a 240 ms latency will also be present.

moving target using the sensors of a remote unit, that 1500 ms latency will make an accurate firing solution impossible; latencies on the order of single milliseconds are required.

d. Low Jitter

Jitter is a measure of the variation of latency. In the case of data networks jitter can be seen in two ways. In the case of streaming data streams such as streaming audio, streaming video, and VoIP, jitter will be seen as a skip in the data stream and is more of a nuisance than anything else. In the case of TCP/IP, jitter can cause packets to become lost requiring the transmitting system to retransmit that packet and potentially leading to the effective transfer rate of the system to significantly decrease. In either case, low jitter is essential for an effective data link.

2. High Availability

As with QoS, high availability of a tactical network is critical. Any network medium used in a tactical network must be available at all times in virtually any environmental condition. It must be able to adapt to dynamic network conditions and quickly provide alternate routing paths in the event a link becomes unavailable.

a. Self-Healing

In the event one of the nodes participating in the network fails, it should have minimal impact on the network overall and the network should quickly be able to re-establish communications with any nodes serviced by the failed node (i.e., find alternate paths.) Self-healing is also a function of the system being routable. In the case of a routed network, when a path from one router to another is disrupted, a router will immediately search for alternate routes to communicate with the destination router. In this case, the loss of a single link has minimal effect on the network as a whole. This is a crucial quality of a tactical network.

b. Centrally and Remotely Manageable

The effective management of a stable and reliable network is rooted in the ability to centrally monitor the health of the network and anticipate failures in the network (Buddenberg). In the case of a tactical network, management of the network is critical in that this function will 1) allow possible failures in the network to be detected allowing for pre-emptive action, and 2) rapid determination of where failures in the network have occurred enabling rapid correction of the failure.

c. Adaptable Transmission Medium

Another factor which contributes to the availability of a wireless system is the transmission mediums ability to adapt to the prorogation environment in which it operates. A wireless radio system must be able to work in virtually any environment while maintaining a stable data link to support applications transmitting and receiving data. In the case of a tactical network, it must be able to operate equally as well in maritime, littoral, and shore-based environments through rain, foliage, dust, etc. The system must be able to automatically adapt to the propagation environment to ensure the maximum bandwidth is achieved by the system.

3. Interoperability

This term implies that all components of the network will function with every other component of the network. However, in the case of information systems, interoperability is a complex matter. Information and communications systems must be interoperable on multiple levels. They must have a medium of transmission that is compatible with other systems, once this has been achieved, they must then have a compatible means of disseminating the information (Info Share 3)[11]. Additionally, once the information has been transmitted to the receiving station, the information must be compatible not only level of data format, but also in terms of data structure. For the purposes of this thesis, interoperability will only be discussed as it pertains to the lower levels of the OSI model.

[11] United States. Department of Defense. Department of Defense Information Sharing Strategy.

With the scope of interoperability narrowed, a ubiquitous tactical networking system must be transparent to the applications that it supports. That is to say if the means of connecting units to the network changes (i.e., wired network, wireless network, etc.) changes, the applications must not be affected by that change. This 1) prevents systems from becoming “stove piped”, 2) allows for seamless switching to new networking means, 3) decreases the cost of upgrading the network as a whole, and 4) increases the likelihood that interoperability will be achieved.

4. Rapid Deployment and Easy Operation

While communicators on ships have adequate time to go through complicated procedures to establish communications with another unit, forces on the ground do not have the luxury of time. Any tactical network used by ground forces must be very simple and easy to use. Additionally, any tactical network must have the ability to be deployed in a short amount of time.

5. High Bandwidth

Bandwidth is a critical factor in the case of a tactical network. In order for information to flow between nodes in a timely manner the network must be able to transport large amounts of information in short periods of time.

6. Inexpensive

The concept of a system being inexpensive must be considered on two levels. The first is the actual unit cost of the system (i.e., the cost of each radio.) The second consideration is the cost of implementing the system into an overall network architecture. Both of these cost factors must be low in order for the system to make economic sense.

7. Security

Any tactical network must have means of securing the data being transmitted over it and ensuring that the data is not modified. Additionally, the system must be compatible with NSA approved encryption methods (i.e., KG-84, KG-175 (TACLANE), etc.) in order to ensure non-compromise of classified information being transmitted over the data links.

C. INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS STANDARD 802.16 FOR LOCAL AND METROPOLITAN AREA NETWORKS

Better known as IEEE Std 802.16, provides for a internationally developed and accepted set of standards for products whose purpose is to provide for long distance, low cost wireless communications in metropolitan areas (IEEE 802.16-2001). Most often the protocol is used to provide “carrier grade” service in “last mile” situations where network service is needed in remote locations. Similar standards have been developed for Wi-Fi (IEEE Std 802.11), which is the most predominant wireless protocol on the commercial market, and wired networks (IEEE 802.3), which is the most predominant network protocol used by the military.

The standard provides for a set of Media Access Controls (MAC) which support multiple Physical Layer (PHY) layer controls allowing the protocol to be able to adapt to a number of environments while maximizing performance. Additionally, the protocol calls for the use of Orthogonal Frequency Division Multiplexing (OFDM) which uses multiple orthogonal sub-carrier frequencies instead of a single carrier frequency to carry data. This use of OFDM has to primary benefits. The first benefit is the ability to carry more data over a given frequency bandwidth than is possible with only one carrier (IEEE 802.16-2001). The second benefit is the waveform’s resilience to interference. In the case of a single carrier an interfering signal is generated, the entire signal is affected. With OFDM, if the same interfering signal is present, only the sub-carrier operating on that frequency is affected, the remaining orthogonal carriers are unaffected and the system remains capable of data transmission (CWNA 197).

The IEEE 802.16 standard allows for the use of Time Division Duplexing (TDD) [IEEE 802.16-2001], the same multiplexing scheme used in TADIL J. As with TADIL J, IEEE 802.16 radios ensure high quality communications, regardless of the number of subscribers, by allocating each subscriber a specified amount of time to transmit and receive data. This also helps to ensure that subscribers do not transmit data at the same time causing packet collisions and forcing the system to retransmit data.

It is important for the reader to understand that if they hear the term “802.16 radios” it does not refer to a single manufacturer or brand of wireless radios.

D. EFFICACY OF IEEE 802.16 BASED WIRELESS COMMUNICATIONS IN TACTICAL NETWORKS

With the discussion requirements of an ideal tactical network and the overview of the IEEE 802.16 standards complete, let us now focus on how IEEE 802.16 based wireless data communications can meet the requirements of a tactical network.

1. Quality of Service (QoS)

Quality of Service (QoS) is a major focus of the IEEE 802.16 protocols. Significant effort is concentrated on ensuring data packets are transmitted and received in a timely manner according to their data types and QoS tags assigned by the host network. In the case of latency and jitter, the IEEE 802.16 protocol uses scheduled services to help ensure that both components are kept to a minimum regardless of the network traffic load. The protocol uses four primary scheduling services in order to achieve low latency and jitter for all data types (IEEE 802.16-2001):

- UGS (Unsolicited Grant Service) – used to ensure efficient transfer of streaming data streams (T1/E1, VoIP, RoIP, etc) with fixed packet sizes.
- rtPS (real-time Polling Service) – used to ensure the efficient transfer of streaming data streams (MPEG, etc) with variable packet sizes.

- ntPS (non-realtime Polling Service) – used to support delay tolerant data streams (FTP, HTTP, etc) for which the packet size is variable.
- BE (Best Effort) – used to support data streams where no minimum service level is required.

For UGS, rtPS, and ntPS, the services use scheduling queues in order to ensure the data is rapidly transmitted to its destination. For BE, the service is a contention based service in which the data is transmitted as space becomes available on the data link.

Due to the protocol specifications contained in the IEEE 802.16, latency and jitter of IEEE 802.16 based wireless radios is very low, even for links spanning hundreds of miles. As an example NPS operates an IEEE 802.16 based data link which links sites at Camp Roberts, CA near Paso Robles, CA to the NPS campus 120 miles to the north. Latency on the data link averages 15-20 ms for a packet round trip; one-way latency averages 7.5 to 10 ms. As will be shown in the next chapter, latency and jitter on sea-based links were consistently measured at 10 – 20 ms.

a. Bandwidth Efficiency

Bandwidth efficiency is a measure of how well a system utilizes the frequency bandwidth allocated for its use to transmit and receive information. Through use of scheduled services and the predominate use of the OFDM waveform in IEEE 802.16 based systems, these radios make efficient use of their bandwidth.

b. Network Determinism

The key to network determinism is the ability of a system to schedule specific time for the data packet to be transferred and a stable means to transfer the data to it’s destination (IEEE 802.16-2001). In the case of IEEE 802.16 based wireless communications, much effort is devoted to scheduling service to each of the subscriber station in the network through the use of scheduling services (as mentioned above) enabling guaranteed data packet handling and traffic enforcement on the wireless network. As a result the services help to ensure that any data packet transmitted on the wireless network is assured delivery in a timely manner.

c. Application Level QoS

At this time no known IEEE 802.16 WLAN radio can prioritize application layer messages on networks, nor does it make good design sense for transmission mediums, such as IEEE 802.16 based radios, to prioritize such messages. The IEEE 802.16 standard does make provisions for systems built in accordance with the standard to recognize traffic priorities based on IEEE Std 802.1q (Quality of Service) and deliver messages based on the priority (i.e., high priority messages are send before low priority messages) [IEEE 802.16-2005]. Many IEEE 802.16 based products, including the Redline AN-80i and Motorola PTP 600 WLAN radios, already employ means for handling application layer 802.1q QoS tags (Redline; Motorola).

2. High Availability

The availability of a wireless network is a function of several factors. While some of these factors are addressed by the IEEE 802.16 protocol, others are external to the protocol and cannot be addressed by it.

a. Routable Networks

The term "routing" refers to an ability to transmit information from a point of origin over a medium, through intermediary nodes, to its final destination. A good example is planning a trip from Los Angeles to New York City. In order for you to get to New York City you need a car, roads to drive on, and driving directions to get there. In this example you are a packet of information, your car is a frame which encapsulates you and carries you from origin to destination, the roads are the medium the data is transferred over (i.e., SATCOM, wireless, wired networks, etc.), the driving directions are routing instructions, and the cities that you will pass through on the way are intermediate nodes. In a simple routing scenario, the path from the origin to the destination is known and always available. In reality, the path a data packet takes is rarely known for certain and a path that was available at one moment in time may not be available the next. In order to overcome this situation routers must be employed to direct packets to their final destination. Think of them as the friendly attendant at the gas station you stop at to ask for directions when you get lost.

In a tactical network where all units are interconnected information must be efficiently transferred from one unit to another. If the path from one unit to another is always the same, a router is not necessary; a bridge is sufficient. However, if the link to that unit fails for any reason, the data must be routed through other routes in order for it to get to the final destination and be of use to the receiving unit.

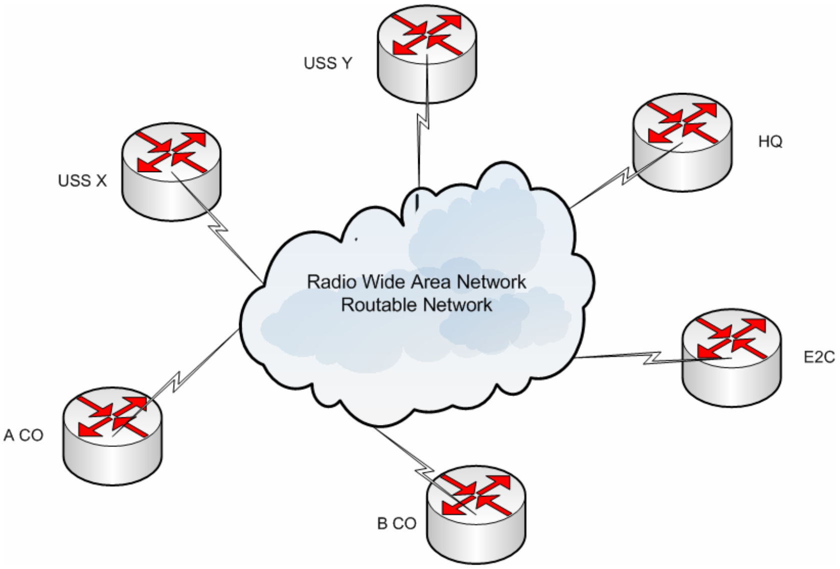


Figure 16 Basic Routable Network.

In a point-to-point data link, radios based on the IEEE 802.16 standard facilitate a dynamically routable network. They act as a medium connecting two networks together allowing data to be transferred from one router to another. In PtMP or mesh data links, the radios will act as “pre-routers”. They will inspect the IEEE 802.16 protocol datagram, determine if it is for the host network or another network wirelessly connected to the radio. If it is for the host network, the radio will send the datagram to the host router. If it not for the host network, the radio will look at its routing table to determine which radio it is for and send it to that radio. In the case of mesh architecture where the destination may be several node hops away, the radio will also determine the best path to get to the destination radio and then send it via that route. In this case of a tactical network, this is a critical function.

b. Robust and Self-healing

In terms of a network, the term “robust” refers to having multiple path of delivering data to its final destination. The term “self-healing” refers to the ability of the network to recover from the loss of one or more nodes and quickly redirect traffic away from those nodes while maintaining service to the other nodes (Buddenberg). When used in PtP links, IEEE 802.16 wireless radios act only as transparent bridges connecting two network nodes together. If the link fails, data will cease to flow. In a PtMP scenario, if a subscriber station (SS) fails, it will not affect the rest of the radio-WAN, thus protecting the overall robustness of the network. However, if the base station (BS) fails, the radio-WAN will completely fail unless one of the SS is capable of taking over the role of the BS.

Mesh architecture is the most robust of all of the radio-WAN architectures (CWNP 318). In the case of a mesh, if one node fails, it will have little effect on the rest of the radio-WAN. The remaining nodes will update their routing tables to take into account the failed node and route traffic around the failed node.

At this time IEEE 802.16 based radios are widely available in PtP and PtMP variants. With the adoption of IEEE 802.16-2005 (Mobile WAN) manufacturers are quickly developing products that will allow for mesh system based on a cellular architecture. Among the suppliers of military systems, both Harris and BAE have products in the final phases of development which are geared to vehicle mounted and handheld IEEE 802.16 based radios. When combined with the dynamic routing capabilities of ADNS, a tactical network immediately achieves the capability of being both robust and self-healing on multiple levels.

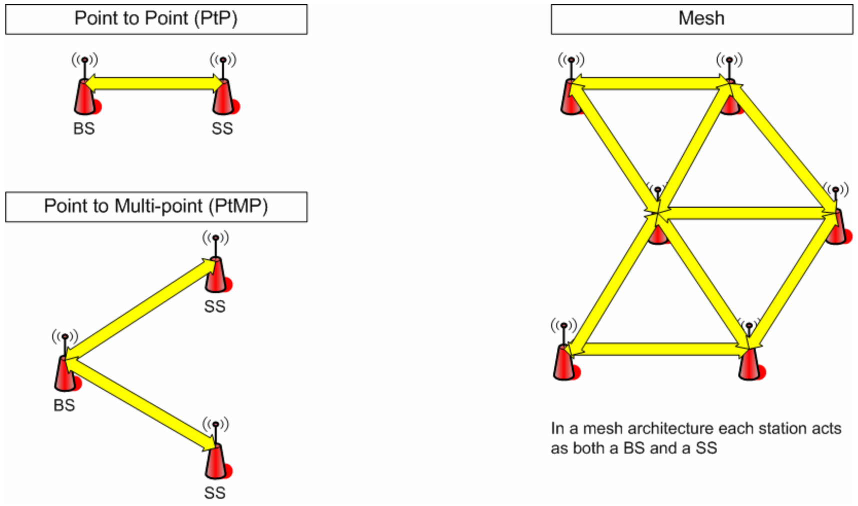

Point to Point (PtP)
BS
SS
Point to Multi-point (PtMP)
SS
BS
SS
Mesh
In a mesh architecture each station acts as both a BS and a SS

Figure 17 Basic Wireless Architectures.

c. *Adaptive Transmission*

The environment that a system operates in cannot be changed; a wireless communications radio must be able to adapt to the environment and changes to the environment. The IEEE 802.16 protocols are well suited, by design, to achieve high availabilities in a multitude of environments through the use of continuous MAC-level link adjustment and the use of OFDM.

(1) MAC-Level Link Adjustments. By design the BS and SS of an IEEE 802.16 based data link continuously exchange information about the quality of the data link they establish (IEEE 802.16-2001). As the environment in which the link is operating changes, the stations detect the changes in propagation and adjust the transmission power of the data link and the modulation scheme of the data link. Adjustments in the transmit power of the radios help them to adjust to changes in the propagation characteristics of the environment (i.e., rain, dust, etc.). Adjustments to the modulation scheme of the data link ensure the maximum amount of data is transmitted over the data link given the environmental factors.

(2) OFDM. As previously discussed, OFDM is ideally suited for environments where RF multi-pathing (dynamic or static) is present. In the event one or more sub-carriers of the OFDM waveform are disrupted, the remaining sub-carriers

will be able to maintain a partial link. In the case of continuous adaptation, IEEE 802.16 based systems continuously monitor the state and "health" of the data link(s) they create. The radios automatically adjust the transmit power of the radio and the modulation of the data in order to achieve the best link possible given the characteristics of the RF environment that the radios are operating in.

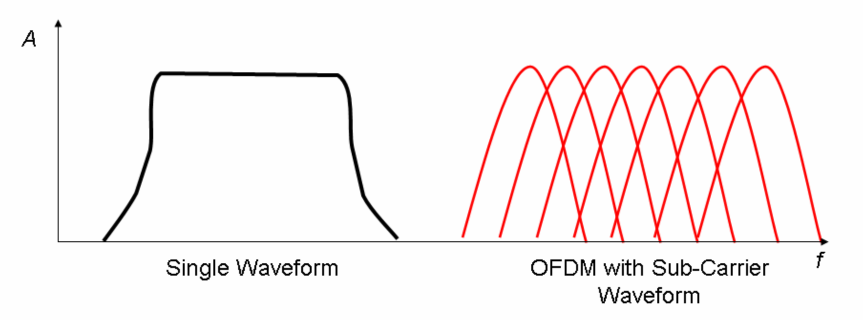


Figure 18 Notional Comparison of Single Carrier and OFDM.

(3) Multiple Input, Multiple Output (MIMO). A recent addition to IEEE 802.16 based product lines is Multiple Input, Multiple Output (MIMO) technology (IEEE 802.16-2005). This technology allows for multiple radios to combine their received signals into a single signal through the use of signal processors. The net effect is the ability to achieve high availability data links in environments where RF multi-pathing is extremely high and effectively combine the throughput of each radio into an aggregate throughput. Hence if a system has four MIMO radios capable of 100 Mbps each, their signal could be combined to form a total throughput capability of 400 Mbps (Sundaresan).

d. Antenna Technology

Antennas are a critical component for achieving a high availability link. However, antenna technology is not a part of the IEEE 802.16 standards. Antenna technology is developed independently of radio technology and is driven by the demands of the market. In the case of IEEE 802.16 based radios, no specific antenna technology has been developed to support them, only generic antennas designed to operate within a given frequency range. In a tactical network, specialized antenna systems will be needed in order to provide high availability links. While the need for such antenna systems is acknowledge, the design of such systems will not be included as a primary point of discussion in this thesis, only general requirements. These issues will be discussed in the "Areas for Further Study" section of this thesis.

e. Centrally Manageable

The idea of central management of a tactical network is critical to the efficient operation of that network. A centrally managed network allows for continuous monitoring of the health of the network, fault isolation, and prediction of failures of the network. The IEEE 802.16 protocols do not directly call for the adoption and usage of any specific network management protocol. However, as the most common and widely used management protocol, the Simple Network Management Protocol (SNMP) is referred to continuously throughout the IEEE 802.16 standards as a "preferred" means of network management (IEEE 802.16-2004). As such, most manufacturers have built SNMP features into their systems allowing for remote monitoring of the network. Both product lines used in to support this thesis research effort were SNMP version 1, 2, and 3 enabled allowing for remote monitoring and management of the systems over long distances. The SNMP protocols were also used to gather the predominance of data used in support of this research effort.

3. Interoperable

As previously stated, this study will focus on interoperability as it pertains only to the lower levels of the OSI model as shown in Figure 19; it will not focus on application level interoperability between systems (i.e., GCCS, TBMCS, etc.). However, it is also necessary to sub-divide this discussion into interoperability between manufacturers and interoperability with networking systems.

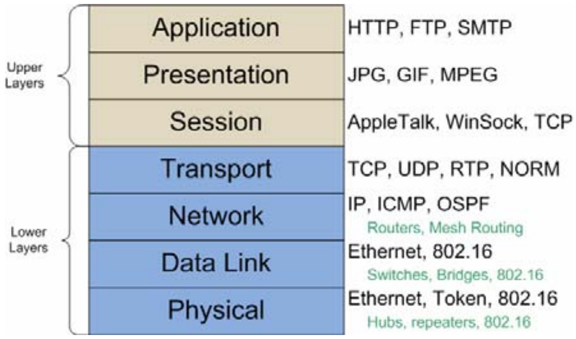


Figure 19 Notional OSI Model.

a. Interoperability Between Manufacturers

Interoperability between manufacturers implies that a radio from one manufacturer will be able to communicate with a radio manufactured by a different manufacturer (Info Share 6). Wireless IEEE 802.11 networking components are, for the most part, completely interoperable thanks to standards developed by the Wi-Fi Alliance[12]. A similar effort is underway to make IEEE 802.16 wireless networking systems compatible, this effort is headed by the WiMAX Forum[13]. Several manufacturers already have "WiMAX" compliant systems and with the adoption of the IEEE 802.16-2005 standard, the number of "WiMAX" compliant manufactures is set to grow quickly. However, interoperability leads to ubiquity, such is the case with Wi-Fi. As the number of compliant components grew, the number of people who had Wi-Fi also grew. While great for the manufacturers it posed a major problem for Wi-Fi security. Due to this fact interoperability on this level is recommended for IEEE 802.16 wireless radios only if they are variants made available only to military operators.

b. Interoperability Between Networking Components

The IEEE 802.16 protocols do not call for physical layer compatibility with any particular physical means of data transport aside from the actual IEEE 802.16

[12] Wi-Fi Alliance develops rigorous tests and conducts Wi-Fi certification of wireless devices that implement the universal IEEE 802.11 specifications.

[13] The WiMAX Forum® is an industry-led, not-for-profit organization formed to certify and promote the compatibility and interoperability of broadband wireless products based upon the harmonized IEEE 802.16/ETSI HiperMAN standard.

transport protocol. As such, it cannot be said that IEEE 802.16 based radios are compatible by design with Ethernet, ATM, etc. However, manufactures have developed IEEE 802.16 based wireless systems that are capable with Ethernet and ATM based networks. For this research effort all of the IEEE 802.16 based radios were completely compatible with Ethernet base networks.

As previously stated, the IEEE 802.16 protocol affects the wireless aspect of the radio only, not the interface to the network. Interfaces to any network type (i.e., Ethernet, ATM, etc.) can be added to an IEEE 802.16 based component without affecting the performance of the radios themselves. Taken in this context, IEEE 802.16 based radios are can be completely interoperable with existing wired networking standards.

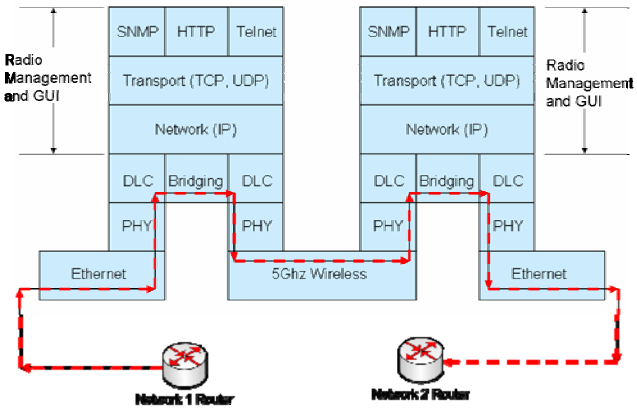


Figure 20 Layer Diagram of Motorola PTP 600 Series 802.16 Wireless Bridge (From: Motorola).

4. Easy to Operate and Deploy

Any communications system used in a tactical network must be easy to use. In the case of IEEE 802.16 based WLAN radios, the ease of use varies from manufacturer to manufacturer and can be considered a function of the maturity of the technology and system architecture used to manufacture the radios. This aspect of the tactical network is not addressed by the IEEE 802.16 standard. However, during the course of this research effort the ease of operation and deployment of the IEEE 802.16 based wireless radios that were used in support of the research were monitored. Both radio systems were operated and managed through graphical user interfaces (GUI) and were simple to operate. As has been noted in past research efforts the most time consuming portion of operating and deploying IEEE 802.16 based radio-WANs is the installation and aiming of the antenna components. Again, these factors are not specifically address by the IEEE 802.16 standards; they must be address through requirement definition and manufacturing.

5. High Bandwidth

As was previously discussed, having adequate bandwidth is critical to the realization of a network centric mode of communications and operations. Without adequate bandwidth, data will not be transferred amongst participating units in a timely manner and will overwhelm the data links used by the units. Since the adoption of IEEE Std 802.16 manufacturers have developed systems that are capable of throughputs ranging from single megabytes per second to over 300 Mbps. As an example, Redline Communications currently offers a product line (AN-80i) which is capable of supporting continuous throughputs of 108 Mbps (Redline). Another product line (PTP 600) owned by Motorola is capable of throughputs up to 300 Mbps (Motorola). Both of these product lines were be used during the research efforts described in the next chapter. In short, IEEE 802.16 WLAN radios can offer throughputs that far exceed any DoD specific wireless communications in existence.

6. Inexpensive

a. Unit Cost

As network centric operations increase in frequency, size, and complexity, the number of nodes connected to a tactical network will increase. If the ultimate NCW goal of making every aircraft, ship, soldier and Marine an node in a network is realized, potentially tens of thousands of radios will be needed. Supplying each node a radio which costs $20,000 is not economically feasible.

With the adoption of IEEE Std 802.16-2005 (Mobile) manufacturers such as Intel have begun the development of IEEE 802.16 based radios small enough and inexpensive enough to place inside laptop computers. While no unit cost is current available for these products, if the model of IEEE 802.11 WiFi is used, unit costs will be on the order of $20. With costs as low as this, it is economically feasible to outfit thousands of nodes with IEEE 802.16 based radios. This is not a suggestion that the same radio used for ground troops will be suitable for use on aircraft or ships. It does, however, illustrate the economy of using IEEE 802.16 based WLAN radios.

b. Implementation Costs

The most expensive portion of any systems acquisition is the installation, maintenance and support of that system. For the purposes of this discussion it will be assumed that based on the predominance of Ethernet and IP based networking technology in military data communications, any IEEE 802.16 based wireless data link will be compatible with these standards. Given this assumption, the implementation costs of an IEEE 802.16 based tactical radio-WAN could be very low as compared to other communication systems employed by DoD. The use of Ethernet compatible radios would make the IEEE 802.16 based radios immediately compatible with ADNS (Johnson). The only addition to the ADNS system that would be required would be the addition of a physical connection to the system and the programming of an addition of data path into the system; for this purposes of this example, a cost of $5000 is assumed per platform. Expanding this to a six ship battle group, a total of $30,000 would be required for modifications to the ADNS system.

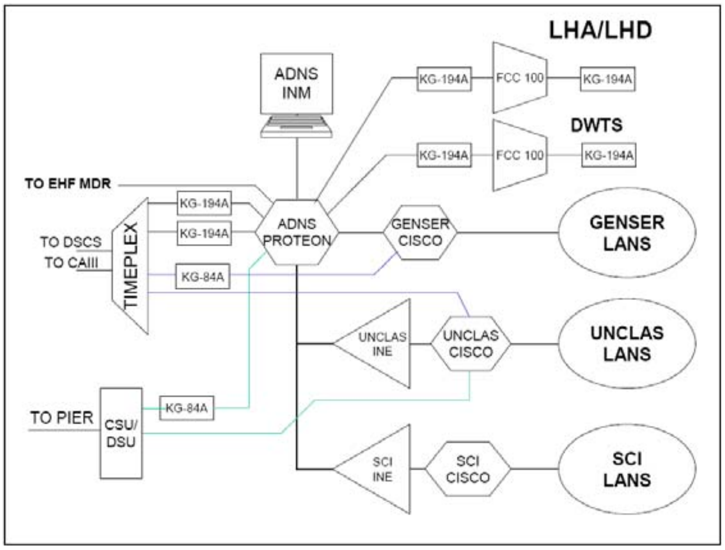


Figure 21 Basic LHD/LHA Shipboard Network (From: ICMC 7-20).

If a PtMP architecture is used using COTS products, is can be accurately assumed that the unit cost of IEEE 802.16 based radios having PtMP, remote monitoring, bandwidths up to 108 Mbps, and organic 128-bit encryption will be $10,000 (Redline). Using these assumptions, the total cost for implementing an IEEE 802.16 based tactical radio-WAN in a six ship battle group would be $90,000.

Given the ease of use of the radios as monitored during this research endeavor, it could be assumed that training on the system would require approximately two hours to complete at $100 per hour of instruction. The one time training of 100 communication technicians for the entire battle group would cost $10,000. In total, the implementation of an intra-Battle group IEEE 802.16 base tactical network capable of bandwidths up to 108 Mbps, high QoS, latencies on the order of 10-20 ms, and immediate compatibility with IP based networks would cost on the order of $100,000.

Admittedly, this example does not take into consideration the total support cost of the system nor the costs associated with realigning ship-board systems to maximize the potential of a battle group based NCW environment. Additionally, it does not address implementation costs of field units on the shore. However, the example does illustrate that in implementation costs of a tactical network based on IEEE 802.16 wireless communications would be relatively low.

7. Security

The IEEE 802.16 standards contain a robust set of organic authentication and data encryption provisions. To ensure that base stations and subscriber stations only communicate with authenticated stations, the IEEE 802.16 standard incorporates two means of authentication into the standards. The first means of authentication is with x.509 certificates based on RSA PKI certificates which enable the base station to authenticate the subscriber station based on the subscriber stations x.509 certificate (IEEE 802.16-2004). If the subscriber station is found not to have a valid x.509 certificate from that link, the base station will not establish further communications with the subscriber station and will ignore further inquiries by the subscriber station.

The second means of authentication adopted by IEEE 802.16 standards is Extensible Authentication Protocol (EAP) [IEEE 802.16-2005]. The same basic authentication procedure described for x.509 authentication is used also for this method.

The protocol also calls for the use of Advanced Encryption Standard (AES) for encrypting data transmitted over the data link. Many manufactures have already built in AES encryption schemes into their IEEE 802.16 based product lines. In the case of the Motorola PTP product lines, AES 128 bit and AES 256 bit encryption schemes are available (Motorola).

Since IEEE 802.16 based wireless radios only act as a data bridge between networks, they are inherently compatible with current NSA approved IP encryptors in use by the military. In basic terms, IP encryptors encrypt the data contained in an IP packet, encapsulate that data into another IP packet and transmit it to its destination where it will be unencrypted and the original IP packet will be routed to its destination. In the case of an IEEE 802.16 data link, another set of encapsulation will take place. The encryptor datagram will be encapsulated in an IEEE 802.16 data gram and forwarded to the destination station. Once there, the packet will be forwarded to the IP encryptor, un-encypted and the original IP packet will be forwarded. An example of this process is shown in Figure 22. If the AES encryption scheme included with the IEEE 802.16 based radio is used, the original datagram is double encrypted using the IP encryptor and the IEEE 802.16 radio.

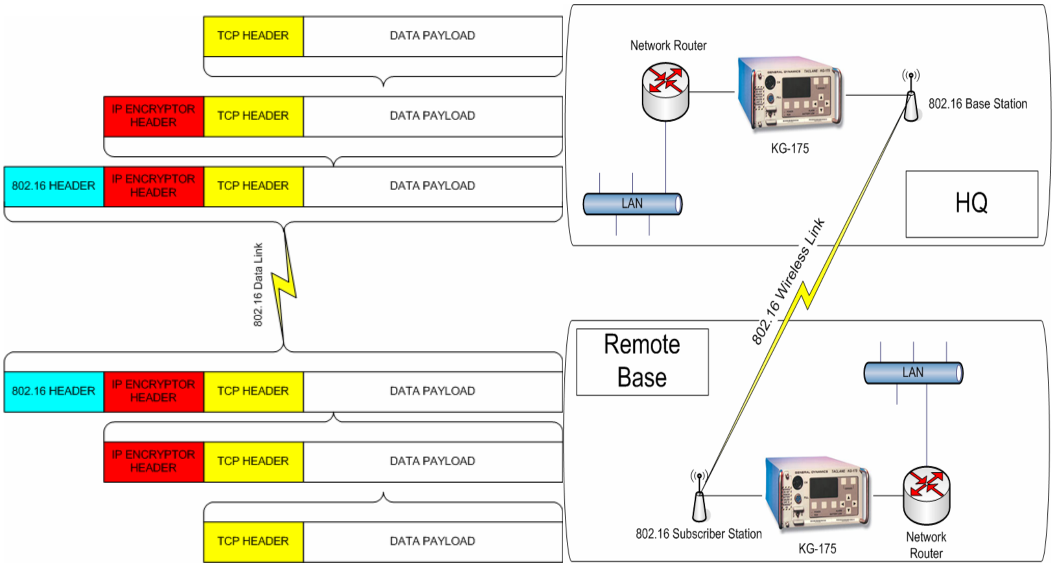


Figure 22 IP Encapsulation.

E. PROPOSED IEEE 802.16 BASED TACTICAL NETWORK ARCHITECTURE

One of the primary tenets of NCW is the interconnection of units within an area facilitating the sharing of information and development of a single, shared common operational picture amongst the units (Alberts et al. 6). With this in mind, Figure 23 illustrates a version of a tactical network which facilitates the NCW concept and in which an IEEE 802.16 based radio-WAN complements both SATCOM and TADIL J communications. The figure shows ships interconnected using IEEE 802.16 based wireless communications systems creating an intra-battle group network which embodies the characteristics of a tactical network.

As well as interconnecting ships at sea, the tactical network can extended to the shore via two proposed paths. The first path is directly from the battle group to the shore using a PTP link. The SS on the shore acts as part of the holonic group on the shore and as a relay to the intra-BG network using shore-based IEEE 802.16 based PtP links. The second path by which the network is extended is through the use of an air-based relay platform (i.e., UAV, E2C, etc.). The aerial platform acts as a relay point for the data link allowing the units on the shore to be connected directly into the intra-BG tactical network. Since the aerial platform is only a relay point, the units on the ground are actually directly part of the intra-BG tactical network. Additionally, since the platform is air-based terrain considerations for establishing LOS data links are eliminated. Another variation of the network would enable the units on the ground to operate as a holonic group in addition to having a link back to the battle group.

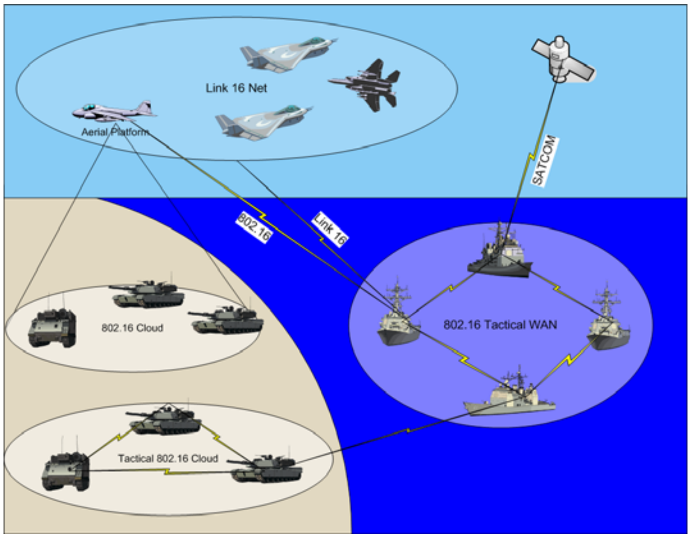


Figure 23 Proposed IEEE 802.16 Complemented Tactical Network.

The proposed tactical network also makes use of existing TADIL J capabilities. TADIL J is a robust and vital communications link and is well suited for air defense operations though it is not directly compatible with IP based systems. While the IEEE 802.16 protocol possesses many of the characteristics of TADIL J, at this time it is not deemed feasible for IEEE 802.16 based wireless communications to replace TADIL J; nor will this thesis attempt to make that assertion. However, in order for units not equipped with TADIL J to benefit from the information and sensors that do use TADIL J, that data must be incorporated into the COP and disseminated to all units in the tactical network. In order to accomplish this, a TADIL J capable unit must act as a broker to translate TADIL J data into routable information. In essence, the unit must act as a translator from the TADIL J data format to an IP-based format using middleware such as the NDDS system developed by Real-Time Innovations, Inc. (RTI)[14] or ComLINK by

[14] Real-Time Innovations, Inc. September 2007, Internet, www.rti.com.

Redondo System, Inc[15]. Once translated, the TADIL J system on the translating platform acts like any other system on a routable network and the information gathered by TADIL J units can be disseminated throughout the battle group and ground forces over the IEEE 802.16 based tactical network.

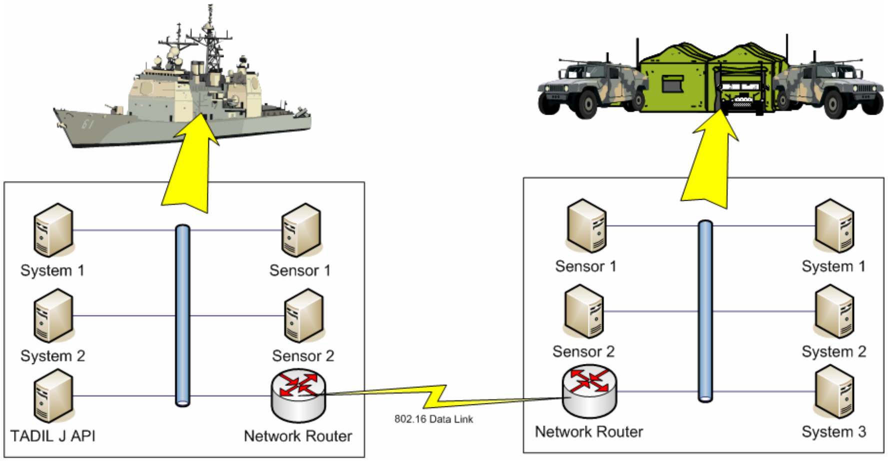


Figure 24 Routable Network Example with TADIL J API.

In order to accomplish beyond the horizon communications the network continues to make use of military SATCOM. However, since communications internal to the area are managed by the IEEE 802.16 tactical network, reliance on SATCOM will be decreased and in the event of SATCOM failure, the battle group will still maintain communication with each other maintaining the integrity of the network.

All of the systems mentioned above can be interconnected using existing systems. Currently ADNS provides multi-data path routing for the IT-21 networks on board naval vessels. Based on previous research endeavors concentrating on the interoperability of IEEE 802.16 based radios and ADNS, both were found to be completely compatible with each other.

[15] Redondo Systems, Inc. September 2007, Internet. www.redondosystems.com.

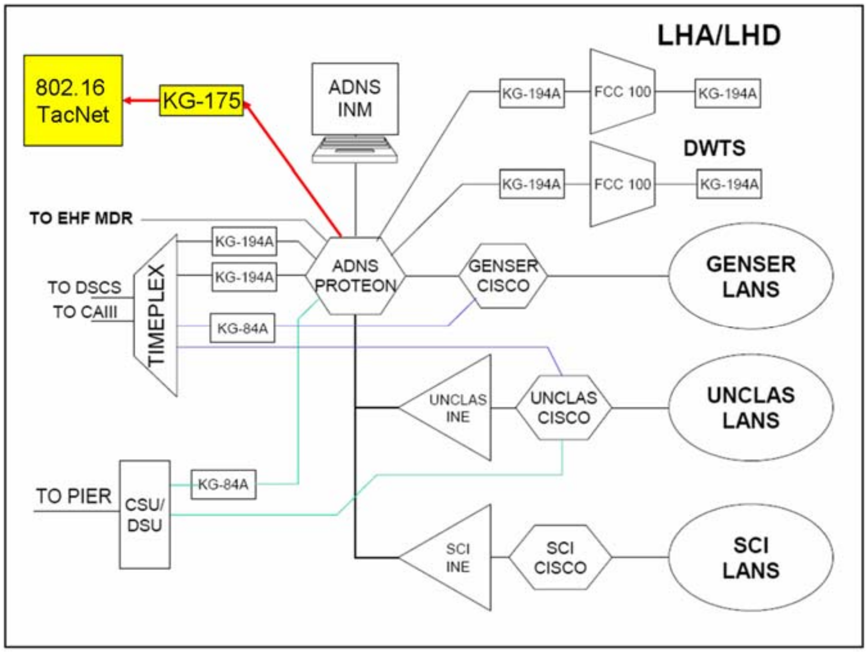


Figure 25 Example Shipboard Network with IEEE 802.16 Tactical Network (From: ICMC 7-20).

F. CONCLUSION

The characteristics of a tactical network discussed in this section only represent a small number of characteristics could be applied to a tactical network. The characteristics that were presented are based on commercial networking “best practices” that can easily be translated into military networks.

From the discussions in this chapter, it can be concluded that IEEE 802.16 based radios have a high efficacy in meeting, or assisting in the achievement, all of the characteristics of a robust tactical network. In addition, IEEE 802.16 based systems have the ability, or can have the ability, to integrate into virtually any IP based networking system. In the case of non-IP based protocols, such as TADIL J, data translators can be used to translate non-IP datagrams into IP datagrams to further extend the range and flexibility of the system in support of NCW based communications.

The tactical network proposed in this discuss is based on commercially available or government available systems already in existence. With minor modifications to existing systems and at relatively low costs, an inter-BG tactical network could be implemented in a matter of months.

In the next chapter, quantitative and qualitative evidence will be presented to further demonstrate the efficacy of employing IEEE 802.16 based wireless radios in meeting the requirements of a tactical network in various shore-based and sea-based network environments supporting the proposed architecture of a tactical network presented in this chapter.

IV. FIELD EXPERIMENTS

A. INTRODUCTION

This chapter will provide a detailed description of the development, implementation and testing of 802.16 based wireless systems used for supporting research for this thesis. At the time of this thesis, military-grade 802.16 wireless data links do not exist. Due to this fact, commercial-off-of-the-shelf (COTS) 802.16 wireless radios were used as substitutes for military-grade systems. None of the systems used during the course of this research is recommended for wide-scale military deployment.

B. TESTS AND MEASUREMENTS

As mentioned, COTS equipment was used throughout the research endeavors supporting this thesis. Performance measurements were accomplished through the use of Simple Network Management Protocol (SNMP) and network traffic generators.

1. Simple Network Management Protocol Data Measurements

SolarWinds v9.0 was used to record system parameters reported by the SNMP agent of the IEEE 802.16 wireless radios used during the experiments. The following parameters were monitored at sample intervals of 10 seconds (unless otherwise noted):

- Received Signal Strength (rxSig)[16]
- Signal to Noise Ratio (SNR)
- Transmit Power (txPow)
- Vector Error (VE [Motorola radios only])
- Transmit Date Rate (TDR)
- Receive Date Rate (RDR)
- Aggregate Date Rate (ADR)

[16] Received Signal (rxSig) is referred to as Received Signal Strength Indicator (RSSI) by Redline. The standard SNMP nomenclature for received signal (rxSig) will be used throughout this document.

- Link Distance
- Free Space Path Loss (FSPL)
- Receive Modulation (rxMod)
- Transmit Modulation (txMod)

2. Network Traffic Simulation

The network analysis software *IX Chariot v6.1* (IXC) was used to generate network traffic in order to measure the characteristics of the IEEE 802.16 wireless data links under simulated network loads. Test scripts based on the IXIA Triple Play test scenario were programmed into *IXC* in order to simulate an asymmetric network traffic scheme in which a user downloads information from a remote source. In this scheme the preponderance of data flows from the remote source to the user; little information flows back to the remote source. The scripts generated the following simultaneous traffic over the date link:

- http (unsecured) traffic – graphics [TCP]
- http (secure) traffic – text [TCP]
- Streaming audio (RealMedia format) [UDP]
- Streaming video (RealMedia format) [UDP]
- Two VoIP G.711u codec (64kbps) phone calls [RTP]
- Duplex IRC chat sessions [TCP]

While data traffic was generated, the following performance characteristics of the IEEE 802.16 wireless data links were measured by *IXC*:

- Throughput (Mbps)
- Latency (ms)
- Jitter (no units)
- Packet Loss (%)

- Voice Delay (ms)
- Total data transmitted in both directions (MB)

3. SNMP Reported Throughput Values versus Actual Throughput Values

Prior to beginning an analysis of individual experiments, it must be noted that the throughput reported by *SolarWinds v9.0* and *IX Chariot v6.1* will be different. This difference is due to the fact that *SolarWinds v9.0* records the total throughput value of the link as reported by the SNMP agent contained within the IEEE 802.16 wireless radio. This reported throughput is the sum of usable throughput for data payload and the throughput available link overhead (MAC layer control frames, etc.) *IX Chariot v6.1* generates data in the application later of the OSI model and thus only reports the usable throughput for data payloads (i.e., TCP, UDP, RTP, etc.). In the case of Motorola PTP 600 wireless bridges, the link throughput, as reported by *IXC*, is consistently 75 – 80% of the SNMP reported throughput of the system. Thus if the SNMP agent reports a link throughput of 100 Mbps, the usable throughput as measured by *IXC* will be 75 – 80 Mbps.

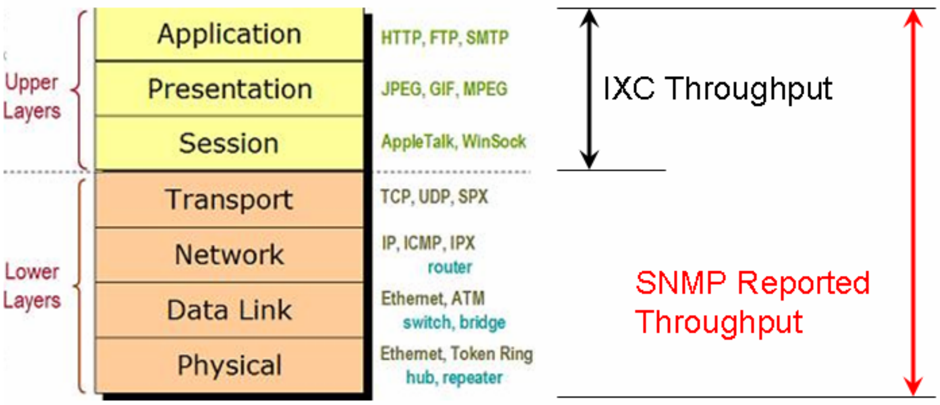


Figure 26 SNMP versus Usable Throughput.

C. EXPERIMENTATION

The primary focus of this research is to demonstrate the efficacy of IEEE 802.16 based wireless data links in supplementing military communications in a cohesive joint networking architecture in various shore-based and sea-based environments. Research was conducted in phases in order to maximize the effectiveness of network architecture design research, testing, and data collection. The phases of experimentation were as follows:

- Phase I - Equipment Familiarization and Initial Testing
- Phase II - Field Trial
- Phase III - Operational Implementation

Several continual field research endeavors at NPS were used to facilitate experimentation conducted in support of this thesis. Two of the primary continuing research efforts used were the Tactical Network Topology (TNT) research initiative and the Cooperative Operations and Applied Science and Technology Studies (COASTS) research program. In addition, several at-sea experiments were conducted in cooperation with the United States Coast Guard Station, Monterey Station using their small squadron of 47 foot motor lifeboats (MLB) and 41 foot utility boats. Final implementation of a prototype IEEE 802.16 based radio-WAN system designed for sea-based operations, which was developed during Phases I and II, was conducted at the Australian Defense Force’s Shoal Water Bay Training Area (SWBTA) north of Rockhampton, Queensland, Australia in support of exercise TALISMAN SABER 2007.

D. PHASE I EXPERIMENTS

1. COASTS FEX I (Monterey Bay)

Initial testing of Redline Communications AN-50 equipment for this thesis research was conducted in conjunction with COASTS Field Exercise I (FEX I) on Monterey Bay in November 2006 in cooperation with the United States Coast Guard, Monterey Station. The purpose of the series of tests was to provide equipment familiarization with Redline AN-50 equipment in a maritime environment, validate datum gather by previous experiments conducted in similar environments, and to determine the maximum link distances achievable using this equipment while maintaining a viable wireless communications link to a base station on the shore. Additionally, the accuracy of the Redline *Link Budget Tool* link calculator was assessed.

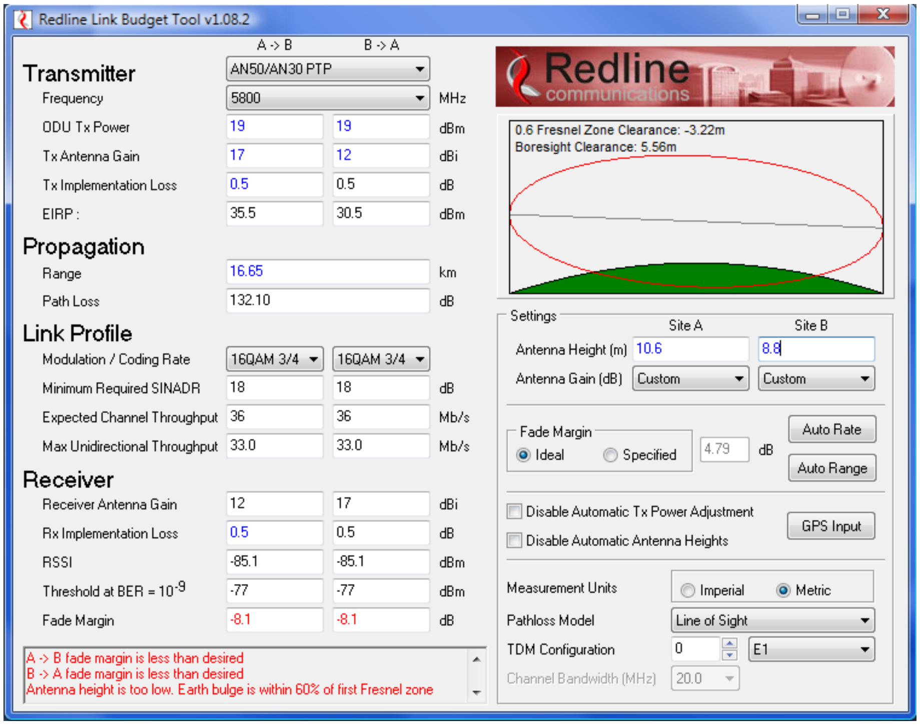
a. Scenario

Aside from data collection, there was no operational scenario associated with this series of tests. The test vessel would perform several data runs over a period of two days in order to gather distance data for the AN-50 data link. During the testing runs the vessel would maintain a constant course and speed in order to minimize the number of variables which may affect the measurements made during the test runs.

b. Measures of Effectiveness and Performance

During this series of test, the primary measure of performance was the received signal strength of the RF link as measured by the subscriber station (SS) on board the test vessel. Throughput was considered, however, it was a secondary measure only.

The threshold for maximum achievable distance was set at a continuous receive signal (rxSig) of -88 dBm (the receive sensitivity (RS) of the AN-50) as measured at the SS on board the test vessel. When the rxSig consistently fell below the RS of the SS, the system would be considered to be at the maximum usable distance. Based on link calculations performed using the Redline *Link Budget Tool*, a maximum distance of 9 nm was to be expected from the data link. The limiting factor of the maximum distance was the height of the antennas of the BS and the SS and earth bulge interfering with the LOS between the two stations.



Redline Link Budget Tool v1.08.2

	A -> B	B -> A	
Transmitter	AN50/AN30 PTP		
Frequency	5800		MHz
ODU Tx Power	19	19	dBm
Tx Antenna Gain	17	12	dBi
Tx Implementation Loss	0.5	0.5	dB
EIRP :	35.5	30.5	dBm
Propagation			
Range	16.65		km
Path Loss	132.10		dB
Link Profile			
Modulation / Coding Rate	16QAM 3/4	16QAM 3/4	
Minimum Required SINADR	18	18	dB
Expected Channel Throughput	36	36	Mb/s
Max Unidirectional Throughput	33.0	33.0	Mb/s
Receiver			
Receiver Antenna Gain	12	17	dBi
Rx Implementation Loss	0.5	0.5	dB
RSSI	-85.1	-85.1	dBm
Threshold at BER = 10^{-9}	-77	-77	dBm
Fade Margin	-8.1	-8.1	dB

A -> B fade margin is less than desired
B -> A fade margin is less than desired
Antenna height is too low. Earth bulge is within 60% of first Fresnel zone

0.6 Fresnel Zone Clearance: -3.22m
Boresight Clearance: 5.56m

Settings

	Site A	Site B
Antenna Height (m)	10.6	8.8
Antenna Gain (dB)	Custom	Custom

Fade Margin: ● Ideal ○ Specified 4.79 dB

□ Disable Automatic Tx Power Adjustment
□ Disable Automatic Antenna Heights

Measurement Units: ○ Imperial ● Metric
Pathloss Model: Line of Sight
TDM Configuration: 0 E1
Channel Bandwidth (MHz): 20.0

Figure 27 Redline *Link Budget Tool* Prediction for Test Series.

c. *Network Topology*

The network architecture used for this series of tests was a simple point-to-point wireless data link. The link base station (BS) was set up at the end of the Coast Guard Pier in Monterey. A single 90-degree 5.8 GHz sector antenna was mounted at the top a 15 foot steel temporary mast and then positioned with the antenna center line facing bearing 350 true and elevation -4 degrees from a zero horizontal plane. The elevation at the pier site was 17 feet AMSL; when added to the mast height of the BS, a total elevation of 32 feet AMSL was achieved.

The subscriber station (SS) was installed onboard a 47 foot USCG motor lifeboat (MLB). The SS base equipment was installed on the starboard side of the pilot bridge of the vessel. A 12 dBm Omni-directional antenna was mounted on a 15 foot temporary steel mast and secured to the starboard, forward stanchion of the pilot bridge. Elevation at the pilot bridge was 18 feet above waterline. When added to the height of the mast, a total antenna elevation of 33 feet was achieved.

Data collection was facilitated by connecting a monitoring laptop directly into the Ethernet port of the SS. The proprietary Redline software *RF Monitor* was used to collect the SNMP data used for the data analysis described later in this section.

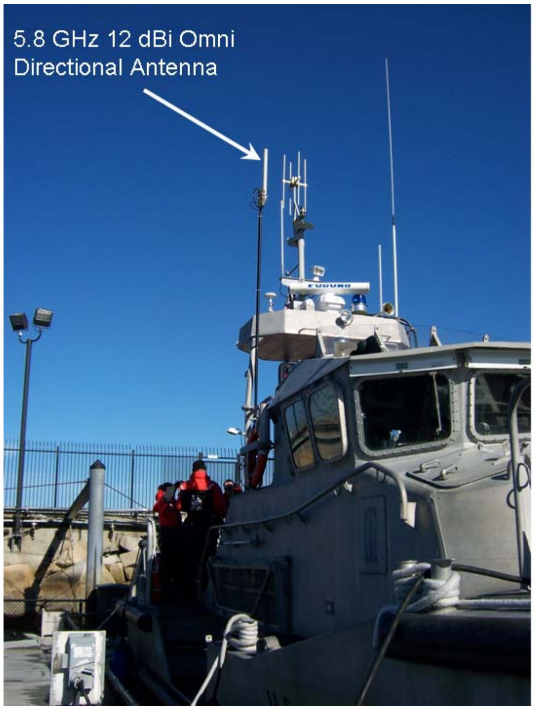


Figure 28 USCG MLB Installation.

d. Test Environment

Throughout the series of data runs, the seas in the area of Monterey Bay that the MLB operated in remained a consistent 4-6 feet wave height with winds of approximately 10 knots.

e. Results

After departing its berth on the Coast Guard pier in Monterey, the MLB positioned itself at a distance of 200 yds off of the pier in front of the BS antenna. The MLB proceeded away from the pier on a course of 350 and speed of 10 kts. Continuous monitoring and logging of the SS rxSig was performed by using *RF Monitor*. Figure 29 depicts the results of the distance testing onboard the MLB. As seen, the data link remained completely viable up to approximately 4 nm. After 4 nm the effects of wave-generated pitch, roll, and yaw on the MLB occasionally caused the rxSig to fall below the -88 dBm threshold causing the link to momentarily drop. Once rxSig rose above -88 dBm, approximately 4 seconds was required for the link to re-establish. At approximately 9.25 nm from the BS, the link became consistently unviable and the test was concluded; similar results were achieved the following day during identical conditions.

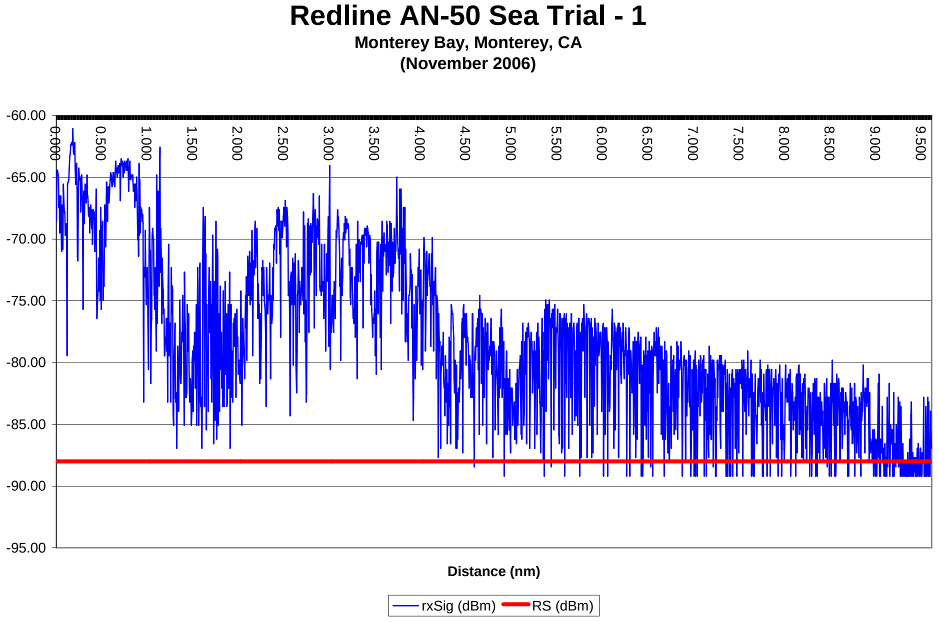


Figure 29 Redline AN-50 Sea Trial Distance Results.

f. Test Conclusions

During this series of tests, results from at-sea experiments previously conducted by other research endeavors were validated. Previous experiments involving AN-50 wireless radios were only able to achieve approximately 4 nm maximum distance while both sets tests for this series of experiments were able to achieve distances of 9.25 nm. It was also noted that the predicted link budget generated by *Link Budget Tool* was fairly accurate in the environment that the test was conducted in. There is no direct means of including factors which affect the free space path loss (FSPL) of the link to increase the accuracy of the link budget, however, the accuracy of the *Link Budget Tool* was considered adequate for future use.

Of particular note are the variations in rxSig evident throughout the data for both days of experimentation. This variation was due to the pitch, roll, and yaw of the vessel and the changing propagation environment caused by wave action and the motion of the test vessel. As seen in Figure 29, rxSig changes by over 15 dBm in a matter of seconds. This rapid, continuous change in rxSig causes the BS and SS to continuously renegotiate PHY and MAC layer parameters to maintain a stable data link. While the link was capable of carrying data, the throughput of the link varied it was not considered a quality link that would be recommended for operational implementation.

2. COASTS FEX II (Fort Hunter Ligett, King City, CA)

The second series of mobile testing was conducted in conjunction with COASTS Field Exercise II (FEX II) in January 2007. Present for this series of tests was the senior technician for the Motorola PTP division, Bob Shaw, in order to provide technical assistance and troubleshooting during the series of test. The purpose of the series of test was to conduct initial familiarization, distance testing, and RF amplifier compatibility testing with the Motorola PTP 600 series of 802.16 radios.

Throughput testing with IX Chariot was not performed during this series of tests.

a. Scenario

Aside from data collection, there was no operational scenario associated with this series of tests. Testing would be done independently of other experiments being conducting in conjunction with COASTS FEX II and would not be incorporated into any scenarios involved with FEX II.

Data collection would be performed over two driving courses and one fixed location. The driving courses would be divided into a vehicle course from the BS to Schoonover Field and then from Schoonover Field to the San Antonio Mission located in the main portion of the base. The fixed location would be at the Site Alpha repeater site on the northern boarder of the Fort Hunter Liggett military reservation. This site was also the furthest accessible site from the site of the BS that was still on the Fort Hunter Liggett military reservation.

b. Measures of Effectiveness and Performance

During this series of test, the primary measure of performance would be the received signal (rxSig) of the SS as measured at the SS. Throughput would be considered, however, it would be a secondary measure only.

The threshold for maximum achievable distance was set at a rxSig of -88 dBm (the receive sensitivity of the Motorola PTP 600 wireless radios) as measured at the SS on the mobile platform. When the rxSig consistently fell below the RS of the SS, the system would be considered to be at the maximum usable distance. Based on link calculations performed used the Motorola *Link Calculator*, a maximum distance of 54 km was achievable by the link based on elevations, transmit power, and antenna selections used for this series of experiments.

c. Network Topology

The test network was constructed as a stand alone system to avoid interference with concurrent experiments being conducted during FEX II and acted as an autonomous network. The network design was based on a simple PtP link architecture using a BS installed at a fixed location and a SS installed on a mobile platform.

The base station (BS) was established at the Bald Mountain radio repeater site (35 53 52.15 N 121 07 41.30 W) on Fort Hunter Liggett. At the site, the average elevation was measured by GPS to be 615 m (2135 ft) AMSL and allowed for an unobstructed view of area. Electrical power was available at the site and was used to power the BS continuously. To maximize the MIMO capabilities of the Motorola PTP radios, polar diversity was achieved by using one 90 degree horizontally polarized and one 90 degree vertically polarized 5.8 GHz sector antenna. The antennas were connected to the BS horizontal and vertical RF output using 10 foot lengths of LMR 400 coaxial RF cable. A 1W 5.8 GHz TDD amplifier was placed inline to both antennas. Both antennas were mounted on a 15 foot mast and tripod and secured to the ground using existing grounding lugs and light duty cargo straps.

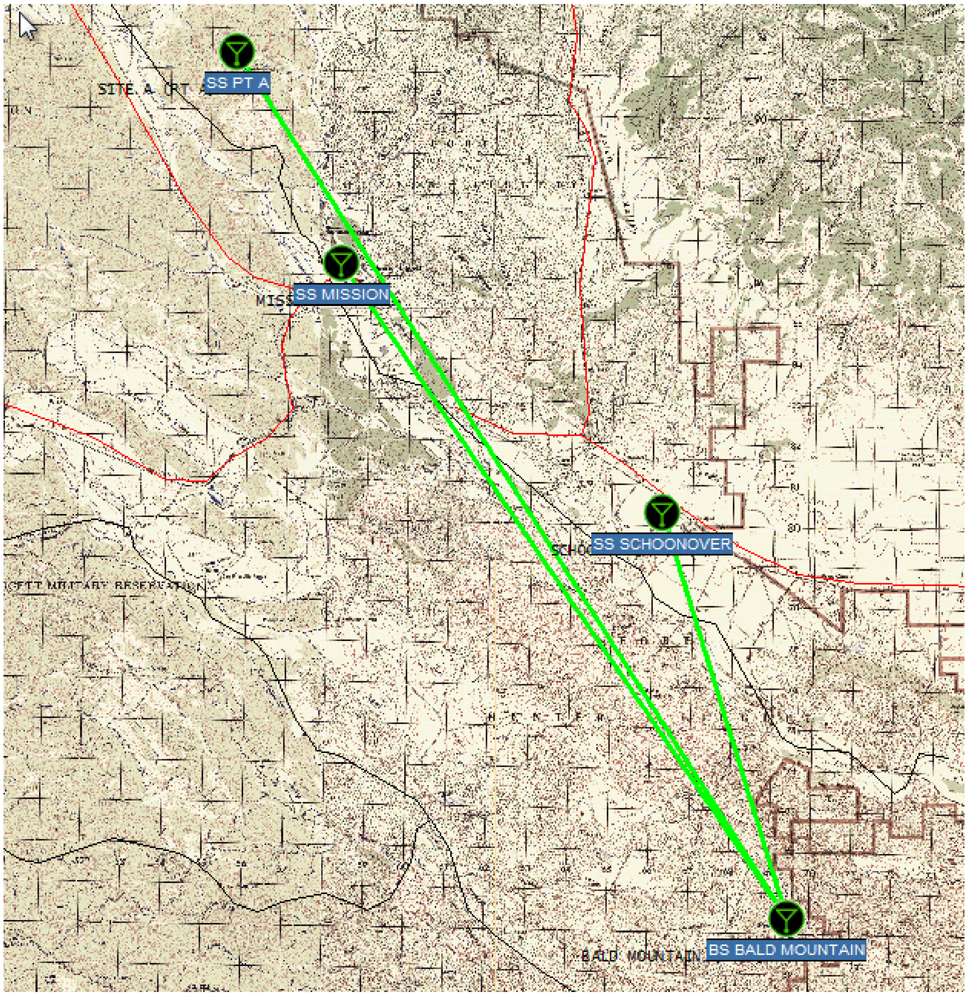


Figure 30 Test Network Topology (FEX II January 2007).

The subscriber station (SS) was installed in the bed of a 2006 Chevrolet Silverado 1500 4-wheel drive. Due the numerous turns that would be required to complete the vehicle course from the BS to Schoonover Airfield, Omni-directional antennas were substituted for the sector antennas used on the BS. One 12 dBi vertically polarized and one 13 dBi horizontally polarized were used as SS antennas. Power for the system was provided by a marine-grade 64 AH gel cell battery connected to an 1100 W AC/DC inverter. Date collection was performed by monitoring SNMP data directly from the radio.

d. *Results*

(1) Bald Mountain to Schoonover Field. From 0 to 14 km from the SS, the terrain was characterized by rolling hills and winding roads with frequent vegetation ranging in heights from 1 to 35 feet. The winding roads and hilly terrain provided an adequate simulation of pitch, roll and yaw that would be encountered in a blue or brown water maritime environment. For reasons of safety, vehicle speed was limited to 20 mph during this phase of mobile testing.

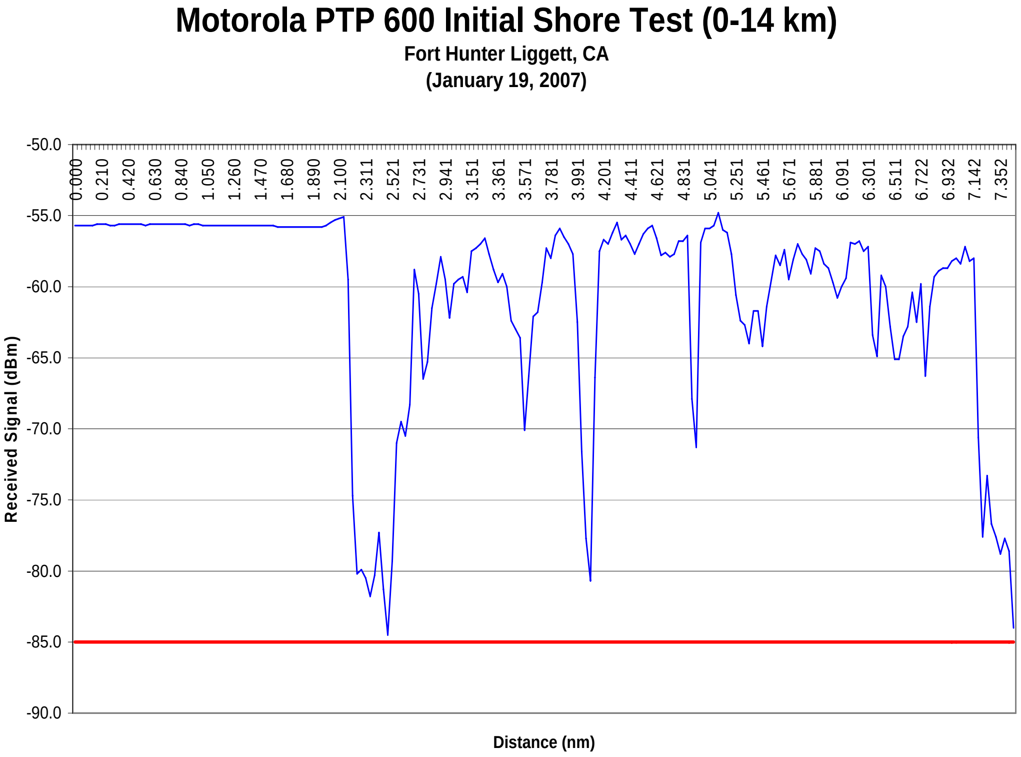


Figure 31 Motorola PTP 600 FHL rxSig (0-14 km).

After establishing a stable link at the BS site, data collection commenced with sample intervals of 2 seconds. As seen in Figure 31 the link remained extremely stable throughout the test run. Various disruptions are seen in the link as distance increases on the chart. These disruptions were due to blockages caused by terrain and dense vegetation.

(2) Schoonover Field to San Antonio Mission. From 14 to 20 km the road was fairly flat with few bends and paved. Due to the good condition of the roads, maximum vehicle speed was increased to 60 mph (maximum posted speed limit of the road.) A maximum distance for this phase of testing was set at 20 km from the BS due a significant change in direction of Mission Road; past this bend the road entered a valley which completely blocked RF reception from the BS.

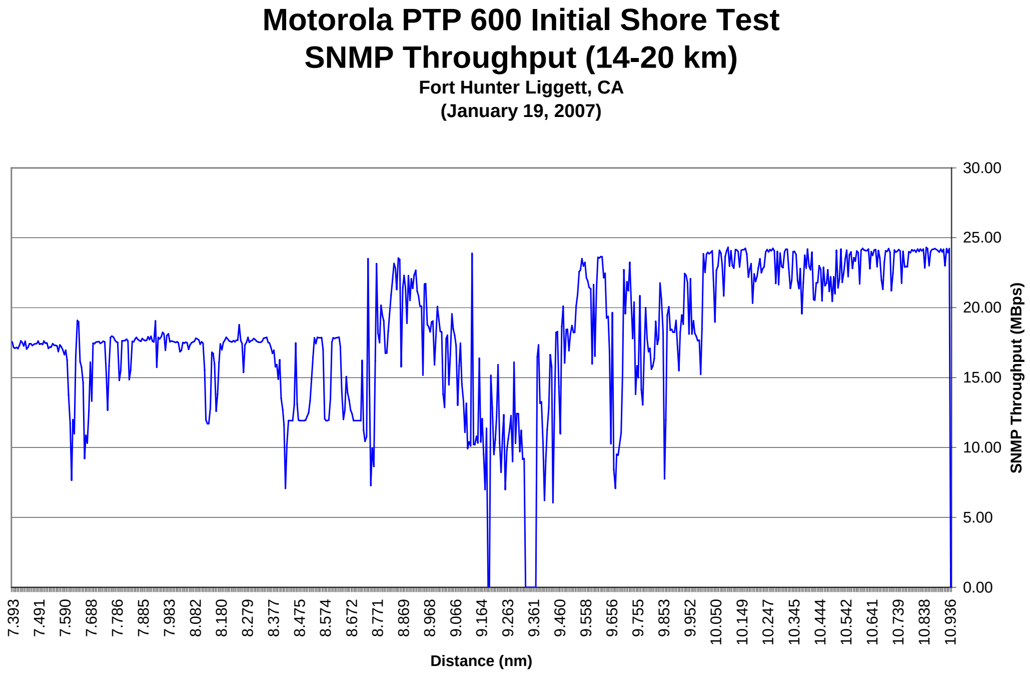


Figure 32 Motorola PTP 600 FHL SNMP Reported Throughput (14-20 km).

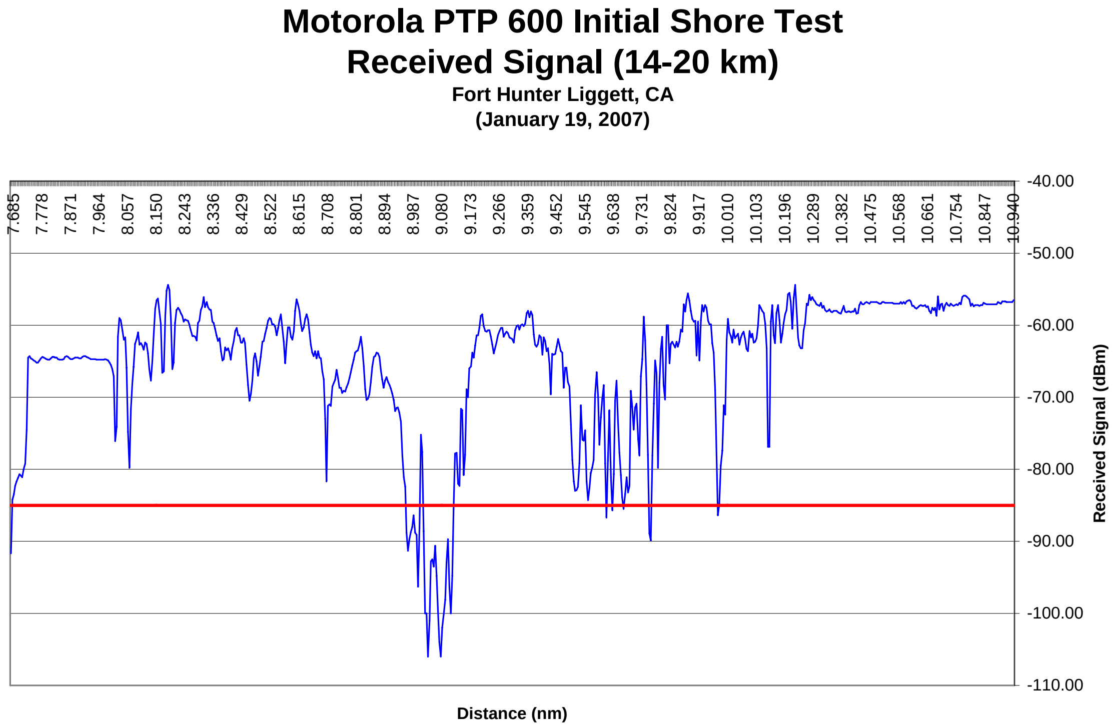


Figure 33 Motorola PTP FHL rxSig (14-20 km).

Four test runs were conducted along Mission Road, only one set data is shown in Figures 32 and 33. A stable link was maintained throughout all four test runs at speeds of 60 mph.

(3) Site Alpha Repeater Site. Due to terrain restrictions the final test was conducted at a single location located 27 km from the BS. This site was the only accessible site with line of sight to the BS location. Results from this test are shown in Figure 34.

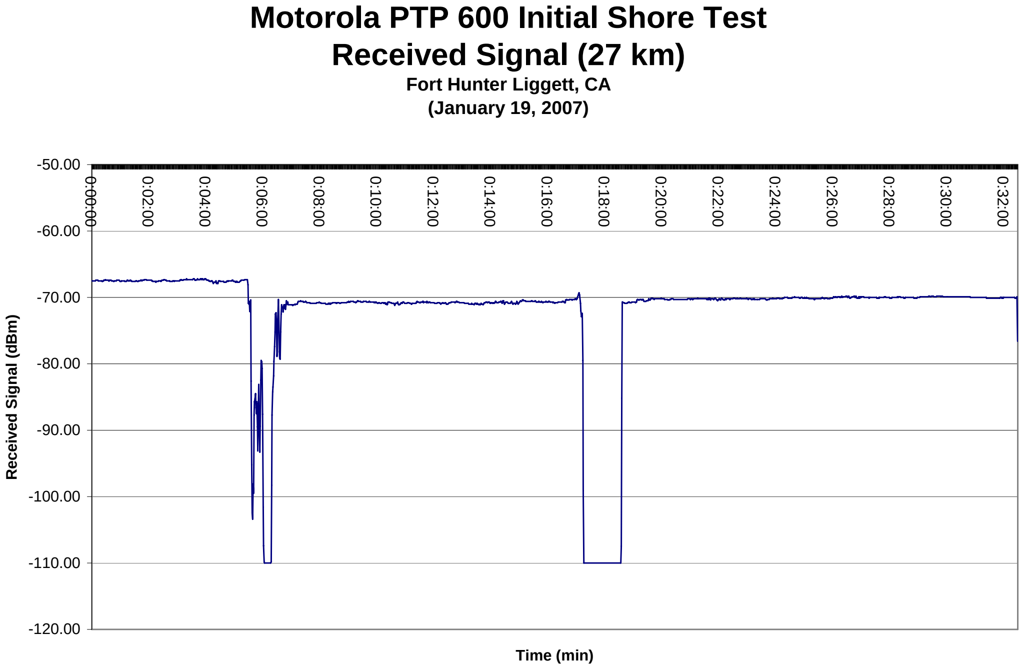


Figure 34 Motorola PTP 600 FHL rxSig (27 km).

e. Test Conclusions

The test series conducted at Fort Hunter Liggett yielded extremely good results and demonstrated the performance of the Motorola PTP 600 radios. As can be seen from the test results, the Motorola PTP 600 radios performed extremely well in mobile conditions over terrain approximating the movement of vessels at sea.

The maximum distance measured during the test series was approximately 27 km. However, as can be seen in Figure 34, the rxSig at that distance was well above the RS of the radios. For this test series, the limiting factor was test range; in essence, the test range did not have sufficient distance in order to measure links greater than 27 km in length.

After the conclusion of the test series, it was discovered that maximum transmit power of the radios was set at 25 dBm. Under normal circumstances this is the normal setting of the radios. However, as part of the test series 1W 5.8 GHz TDD amplifiers were installed on both radios to test the compatibility of the radios with power amplifiers. This power setting exceeded the maximum input power of the amplifiers. The radios were able to automatically reduce their power output to 15 dBm, the OFDM waveform was clipped reducing the maximum available throughput of the links. In order to avoid clipping the OFDM waveform, the maximum power output of the radios should have been set to 10 dBm (a power "back off" of 5 dBm.) While the radios function well up to the maximum tested distance of 27 km, had the error in power settings been caught during the test series, the throughput of the link would have been much greater than the throughputs recorded during the test series.

3. USCG Testing (February 2006)

To validate test results achieved at Fort Hunter Liggett and to test the Motorola PTP 600 radios in a maritime environment, at sea testing was coordinated with the Commanding Officer of USCG Station Monterey. Additionally, distance testing up to 10 nm (maximum distance predicted based on LOS considerations) would be attempted, seas permitting. The test series was conducted in two test runs over a period of two consecutive days.

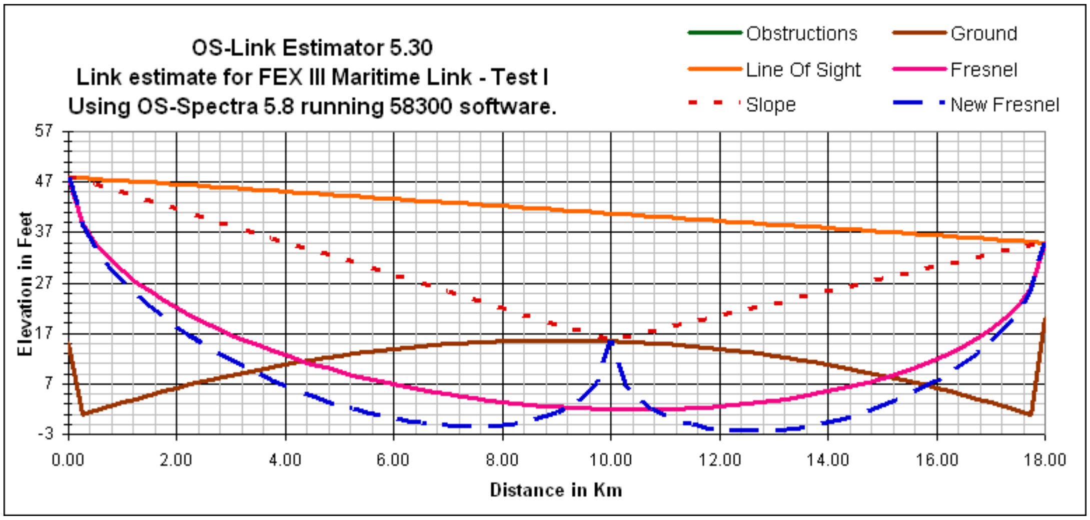


Figure 35 Motorola PTP 600 Predicted Link Profile for USCG Testing.

a. Scenario

Aside from data collection, there was no operational scenario associated with this series of tests. The test vessel would perform several data runs over a period of two days in order to gather distance data for the IEEE 802.16 data link created by the Motorola PTP 600 wireless radios. The vessel would perform constant course and speed runs during all test series.

b. Measures of Effectiveness and Performance

During this series of test, both rxSig and SNMP throughput would be the primary measures of performance. Both *SolarWinds v9.0* and *IXC* were used for data collection.

c. Network Topology

The NPS mobile research vehicle "NEMESIS"[17] was used to establish a base station at the NPS Maritime Research Facility on the shore of Monterey Bay by NPS. The BS radio was mounted on a 40 foot telescoping mast attached to NEMESIS. An antenna configuration identical to the one used during the tests conducted at Fort Hunter Liggett was used for the BS antenna configuration. Once mounted, the BS was raised and set to an azimuth of 350 degree (magnetic.)

The SS was installed on the pilot bridge of USCG Station Monterey's 47 foot MLB. On the pilot bridge, two 90 degree sector antennas were mounted on a 15 foot mast attached to the starboard, forward stanchion using three metal binding straps. The antennas were pointed Aft (180 relative bearing) to provide aft RF coverage as the test vessel opened on the BS. The SS was connected to a 1U 24 port rack-mounted switch mounted inside of a water resistance portable rack. Additionally, an 1100W AC/DC inverter was mounted inside of the case to provide power to the components of the system. Power for the system was provided by a 64 Ah marine-grade gel cell battery.

[17] NEMSIS is a 33 foot Class A recreational vehicle converted by NPS staff and students to be a mobile networking platform.

Both *SolarWinds v9.0* and *IXC* were used for data collection during the test run. Two laptop computers, one with *SolarWinds v9.0* and other with IXC, were connected to the 24 port switch on the test vessel in order to collect SNMP and perform network stress testing.

d. Results

Due to heavy weather and high seas on Monterey Bay, Day 1 of testing was cancelled for reasons of safety. The following day, the weather and seas eased sufficiently to allow for testing to commence.

Day 2 of testing commenced with the MLB getting underway from the Coast Guard Pier in Monterey in route to the NPS Marine Research Facility (MRF). Upon arrival, the MLB was positioned at a distance of 1000 yds from the shore in front of the MRF. Once the data link was established and data collection commenced, the MLB proceeded away from the shore on a course of 350 and a speed of 10 kts. Seas close to shore were approximately 4–5 feet with a wave period 7–10 seconds. As the test progressed, weather conditions quickly deteriorated. At 5 nm from shore, seas increased to 8–12 feet and winds to 15-20 kts. As the seas continued to deteriorate the pitch and roll rate of the MLB increased to the point that the metal bindings used to install the mast to the pilot bridge failed causing the 802.16 antenna system to fall onto the aft deck of the MLB, narrowly missing two crew members. Conditions onboard the MLB would not allow repairs to the antenna system while underway and the remainder of the test run was cancelled.

e. Test Conclusions

Despite the loss of one full day of testing and the early termination of the second day of testing due to weather and seas, the test series yielded significant results. As seen in Figure 36, the stability of rxSig was much improved over the results previously seen using the Redline AN-50 radios. This link stability allowed for a much more stable SNMP throughput and usable throughput. Table 1 summarizes the IXC results from the data set taken at 4 nm on board the MLB in 8 – 10 foot seas with a rapid pitch and roll rate. The improvement in rxSig and throughput is attributed to the performance gain achieved by using the MIMO technology that is part of the Motorola PTP radio set.

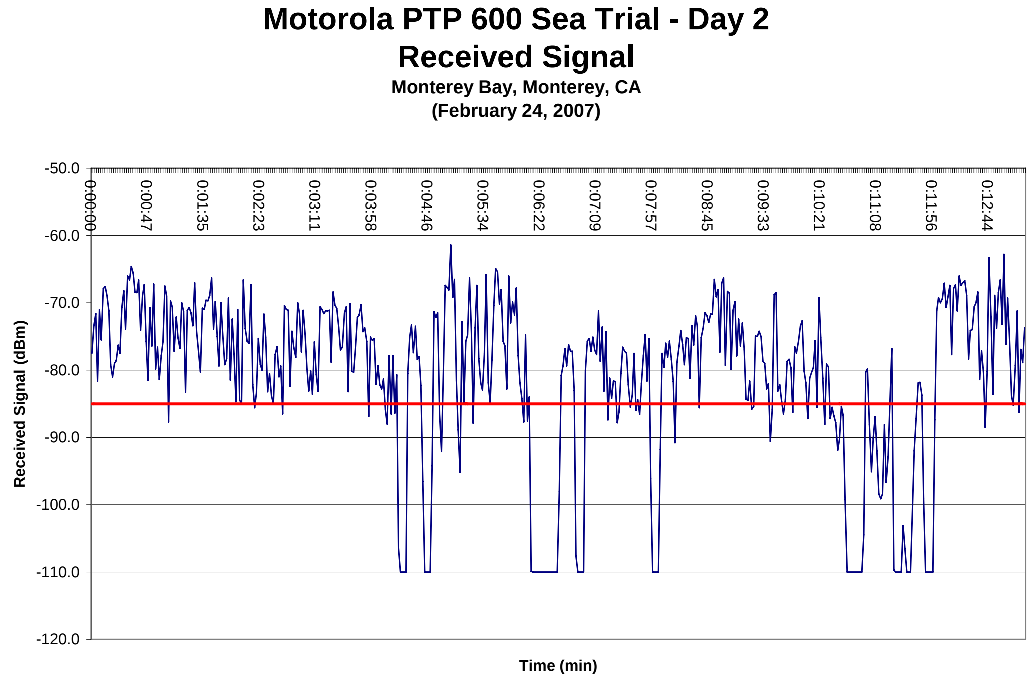


Figure 36 Motorola PTP 600 USCG rxSig (Sea Trial Day 2).

FEX III IX Chariot Data Summary								
Distance (nm)	Throughput (Mbps)			VOIP MOS	One-way Delay (ms)	Lost Data (%)	Jitter (ms)	Bytes Sent (MB)
	Receive	Transmit	Total					
1	17.044	24.088	40.011	4.37	5	0	3.55	306.500
2	1.808	3.835	5.881	1.59	6	27.1	2.47	46.264
3	6.060	18.006	28.216	6.87	11	1	3.30	275.560
4	3.087	5.260	7.920	2.37	10	1.5	12.80	61.090

Table 1 FEX III IX Chariot Data Summary.

This test series also showed the advantage of using two antennas in a MIMO system. In addition to tolerating a more dynamic RF environment, the use of two antennas allowed for greater range of vertical RF coverage by adjusting the vertical tilts of the horizontal and vertically polarized antennas. The vertical beam of both antennas was 8 degrees. In a single radio system this would cause the SS to lose RF connection to the BS when the vessel experienced a pitch and/or roll greater than 4 degrees from a zero plane. However, by using two antennas, one antenna can be adjusted to +4 degrees from a zero plane and the other antenna adjusted to -4 degrees from a zero plane allowing for 16 degrees of vertical beam coverage thus enabling the vessel to experience pitch and/or rolls of up to 8 degrees from a zero plane without loosing RF connection to the BS. While a 16 degree coverage (+8/-8) coverage is a significant improvement over previous experiments, the MLB experienced pitches and rolls of up to 20 degrees during the test run.

E. PHASE II EXPERIMENT - TNT 07-02 MARITIME INTERDICTION OPERATION (MIO), SAN FRANCISCO BAY

The first field implementation of the array system developed as part of this thesis research was done in conjunction with TNT 07-02 MIO in San Francisco in March 2007. This series of tests would test the systems ability to maintain a stable wireless data link on board a medium sized vessel in deep water conditions out to 10 nm from shore .

1. Scenario

The scenario for TNT 07-02 MIO was the detection and interception of a vessel in bound to a U.S. port with a nuclear dirty bomb on board. The detection of the vessel would occur at 12 nm from U.S. territorial water. As the vessel approached SF Bay, law enforcement vessels would be dispatched to intercept and board the vessel. Once on board, law enforcement agents would search the vessel for persons of interest and attempt to locate and identify the nuclear materials held on board the vessel. Readings from hand held radiation detectors would be uploaded to a central laptop and transmitted by the wireless link to Lawrence Livermore National Laboratory (LLNL) for analysis while the vessel was still at a safe distance from shore. In this scenario, the MV Pacific Responder[18] would act as the vessel of interest carrying the dirty bomb. The wireless

[18] MV Pacific Responder is a 210’ environmental emergency response vessel operated by Marine Spill Response Corporation and homeported Port Richmond, CA.

data link provided by the Motorola PTP 600 system would provide the wireless network link enabling law enforcement communications and data transfer to and from the vessel.

2. Environment

During the test series, seas were from the West at heights of 12- 15 feet 1 nm off shore with a period of 8 – 10 seconds.

Figure 37 MV Pacific Responder.

3. Network Topology

Once established, the Motorola PTP 600 radio-WAN would be linked into the TNT experiment network established in the San Francisco area. This metropolitan area network (MAN) links multiple sites around the San Francisco Bay area using Redline AN-50 5.8 GHz radios using multiple PtP data links. Additionally, the MAN is connected to the NPS CENETIXS laboratory using a NPS created VPN connection through commercial internet service providers. The TNT network is also extended 72 miles south of NPS to Camp Roberts, CA, near Paso Robles, CA, using series of Redline AN-50 5.8GHz wireless radios.

The SS was installed onboard the MV Pacific Responder on the signal bridge as shown in Figure 38. The location of the antenna system allowed for almost a 360 degree coverage, however, the main mast of the vessel blocked RF coverage from a relative bearing approximately 230 to 250. One element of the array was removed to allow for unobstructed rotation of the ship's Furuno navigation radar. The elevation at the site of installation was measured to be 52 feet above waterline. Taking into account the 10 foot mast used to hold the antenna array, a site elevation of 62 feet was achieved.

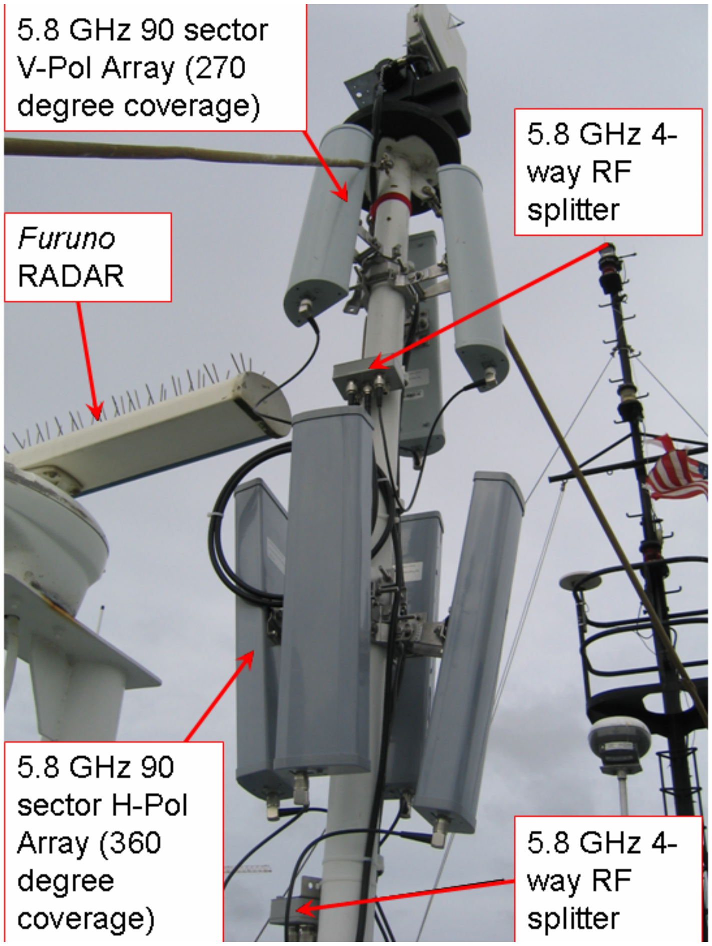

5.8 GHz 90 sector V-Pol Array (270 degree coverage)
5.8 GHz 4-way RF splitter
Furuno RADAR
5.8 GHz 90 sector H-Pol Array (360 degree coverage)
5.8 GHz 4-way RF splitter

Figure 38 5.8 GHz Antenna Array as installed on MV Pacific Responder.

The BS was installed on top of the Golden Gate Bridge administration offices on the San Francisco side of the Golden Gate Bridge (GGB). The elevation on top of the office was 189 feet above mean sea level (AMSL.) The BS was installed on a 15 foot mast attached to mechanical housing on the roof allowing for a total mast height of 204 feet AMSL. One horizontally polarized and one vertically polarized 90 degree 5.8 GHz sector antenna was used for RF coverage of the western approach to San Francisco Bay as seen in Figure 39. Coverage was not provided inside of the bay to prevent interference with 802.16 wireless links installed around San Francisco Bay as part of the TNT MAN.

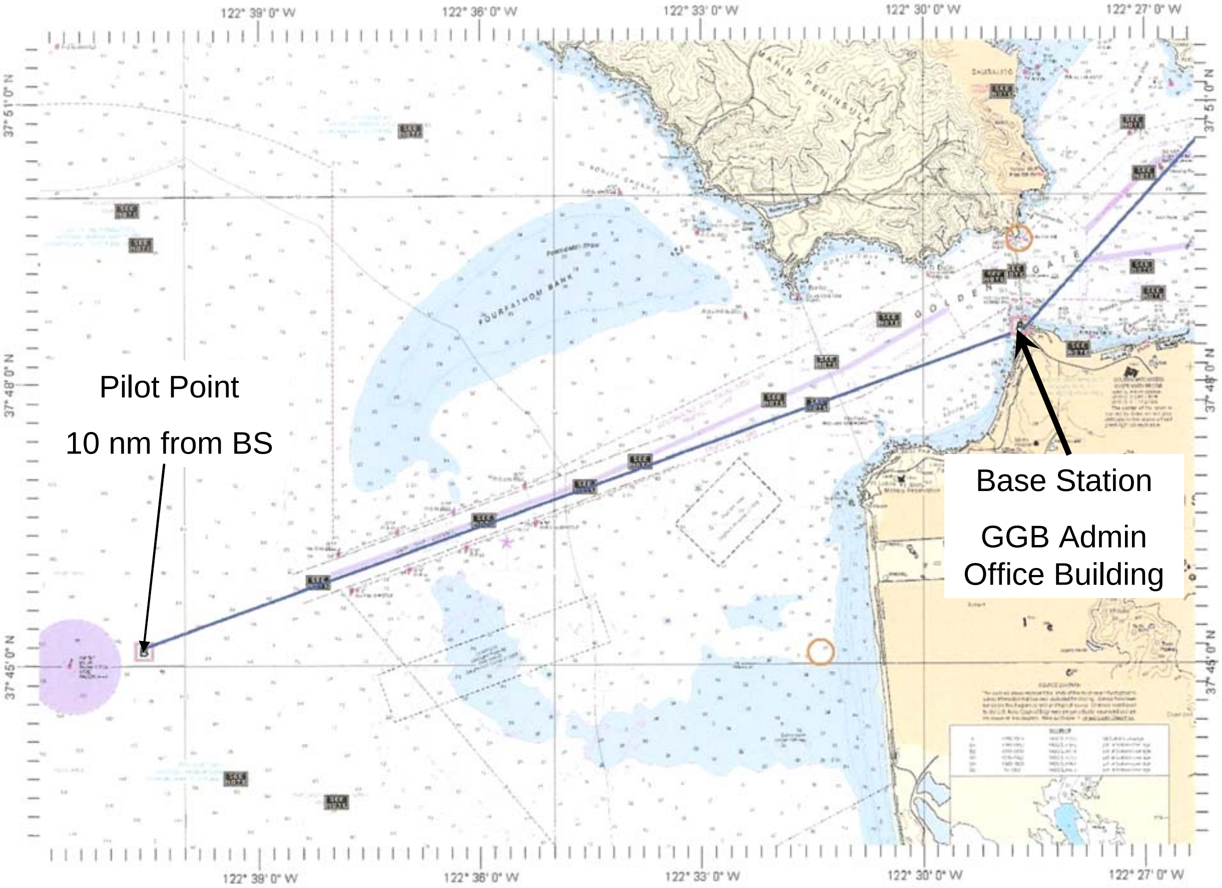


Figure 39 TNT 07-02 MIO Test Route.

4. Testing

Once underway, the vessel transited to the GGB in route to Pilot Point, a location 10 nm west of the GGB. After passed under the GGB, the SS on the Pacific Responder established a link with the BS on the GGB administration offices. At approximately 2 nm from the GGB, the vessel began encountering heavy and increasing seas. The vessel’s course along the outbound vessel transit lane took it directly into the seas which caused significant pitching (+15/-15 degrees), but negligible roll and yaw. The rxSig and

SNMP throughput results from the establishment of the link at 1 nm to the terminal point at 10 nm are shown in Figure 40. As seen in the figure, wave action played a significant role in the stability of the link during the outbound transit. As the changes in pitch of the vessel increased beyond the +8/-8 degrees of the antennas array’s vertical coverage, the stability of the link decreased as the link experienced outages due to not being able to maintain a RF connection with the BS. However, when the vessel was able to maintain a pitch of +8/-8 and below, the link was able to achieve an average SNMP throughput of 100 Mbps. No IXC testing was performed during the outbound leg due to the instability of the link.

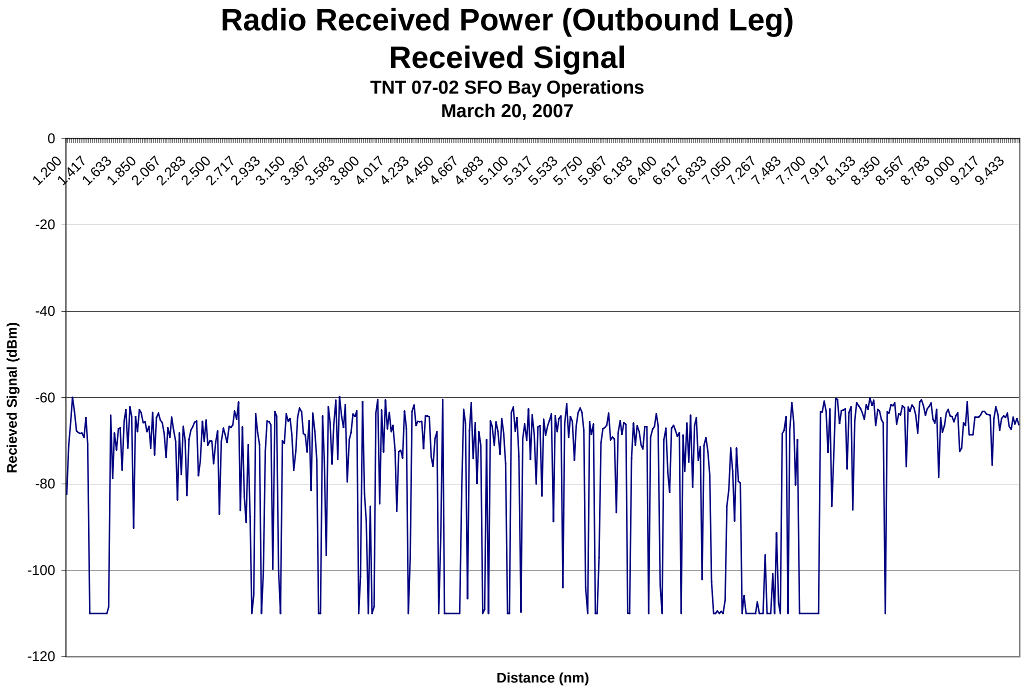


Figure 40 TNT 07-02 Outbound Received Signal.

At 10 nm from the GGB, the vessel turned and began transiting back into SF Bay. From 10 to 8 nm the vessel’s speed was adjusted to more closely match the speed of the waves. With the speed adjusted and with following seas, the pitch of the vessel was an average of +5/-5 degrees for the remainder of the transit in. This platform stability is seen in Figure 41.

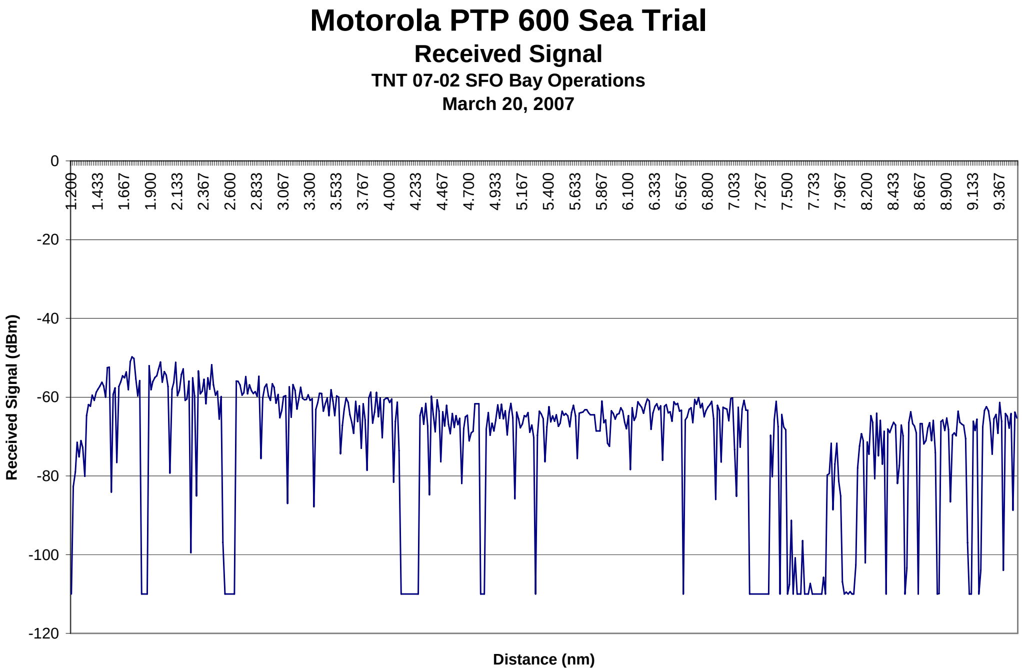


Figure 41 TNT 07-02 Motorola PTP 600 Received Signal (Inbound Leg).

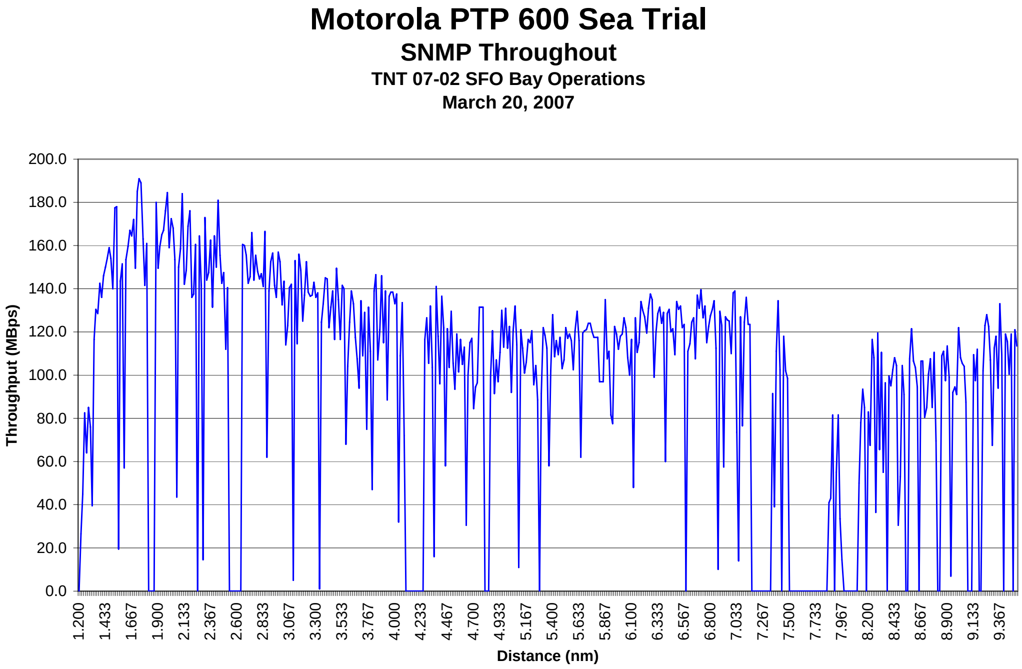
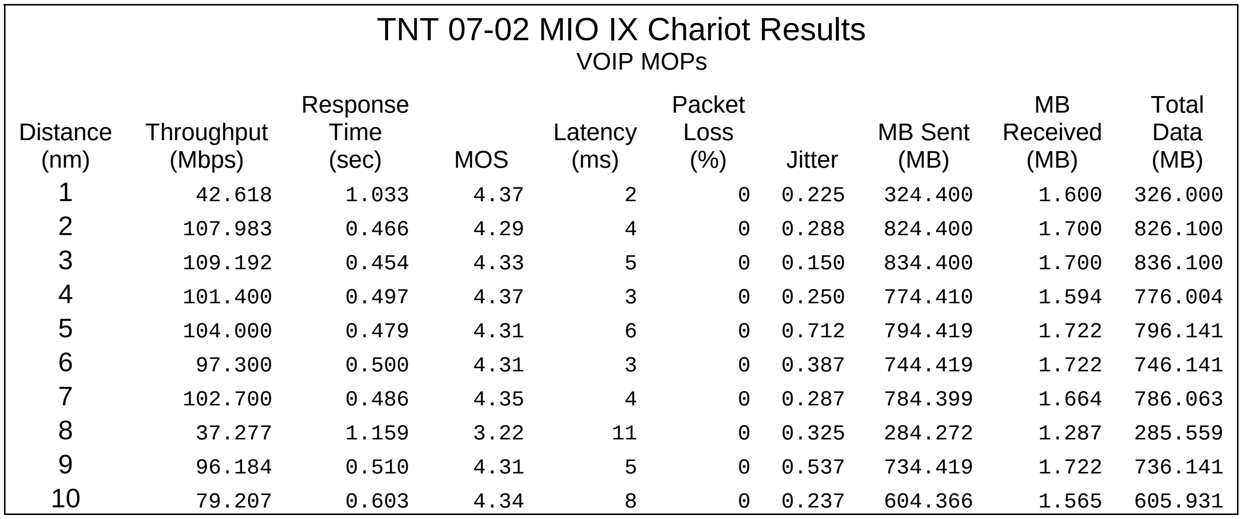


Figure 42 TNT 07-02 Motorola PTP 600 SNMP Throughput (Inbound Leg).

This graph shows that rxSig stabilizes at approximately 7 nm and remains fairly stable from 7 to 1 nm. Throughputs of 80 to 115 Mbps were achieved from 8 to 10 nm, however, once pitch decreased to less than 8 degrees, stable throughputs of 110 – 120 Mbps were achieved. As the vessel approached 3 nm, throughputs increased from an average of 120 Mbps to a maximum of 185 Mbps. Link availabilities of over 98% were seen throughout the test run.

Table 2 shows a summary of IXC generated data during the inbound leg. Each test was run over a one minute period and usable throughputs of to 109 Mbps were measured. Latency for all *IXC* tests was extremely low; similar to latency numbers that would be experience on a wired local area network. Additionally, the maximum jitter measured by *IXC* VOIP tests was 0.712 ms. File transfers (including TCP, UDP, and RTP) of up to 836 Mbps were accomplished during the inbound leg.



TNT 07-02 MIO IX Chariot Results

VOIP MOPs

Distance (nm)	Throughput (Mbps)	Response Time (sec)	MOS	Latency (ms)	Packet Loss (%)	Jitter	MB Sent (MB)	MB Received (MB)	Total Data (MB)
1	42.618	1.033	4.37	2	0	0.225	324.400	1.600	326.000
2	107.983	0.466	4.29	4	0	0.288	824.400	1.700	826.100
3	109.192	0.454	4.33	5	0	0.150	834.400	1.700	836.100
4	101.400	0.497	4.37	3	0	0.250	774.410	1.594	776.004
5	104.000	0.479	4.31	6	0	0.712	794.419	1.722	796.141
6	97.300	0.500	4.31	3	0	0.387	744.419	1.722	746.141
7	102.700	0.486	4.35	4	0	0.287	784.399	1.664	786.063
8	37.277	1.159	3.22	11	0	0.325	284.272	1.287	285.559
9	96.184	0.510	4.31	5	0	0.537	734.419	1.722	736.141
10	79.207	0.603	4.34	8	0	0.237	604.366	1.565	605.931

Table 2 TNT 07-02 Inbound IX Chariot Summary.

Unfortunately, little actual data was passed during either the outbound or inbound leg. While a radio-WAN connection was available from the vessel to the shore, the TNT MAN experienced RF interference from external sources caused the MAN to become unstable.

5. Test Conclusions

The TNT 07-02 series of experiments were a complete success with respect to the Motorola PTP 600 system ship to shore communications. Results achieved during the test series closely matched the predicted throughputs and received signals generated by the link calculator. This series also proved the viability and the readiness of the prototype array system to be deployment more demanding scenarios.

Unfortunately time constraints of the vessel limited the maximum distance of the data link. In order to support the operational schedule of TNT 07-02 MIO, the vessel only had enough time in the schedule to support distances of 10 nm from shore. As can be seen in Figure 43, the maximum predicted distance of the link was 37 km (20 nm.) Had the Pacific Responder had enough time in its schedule to transit to 37 km from shore it is highly likely that a stable data link could have been maintained given the excess rxSig measured at the 10 nm point.

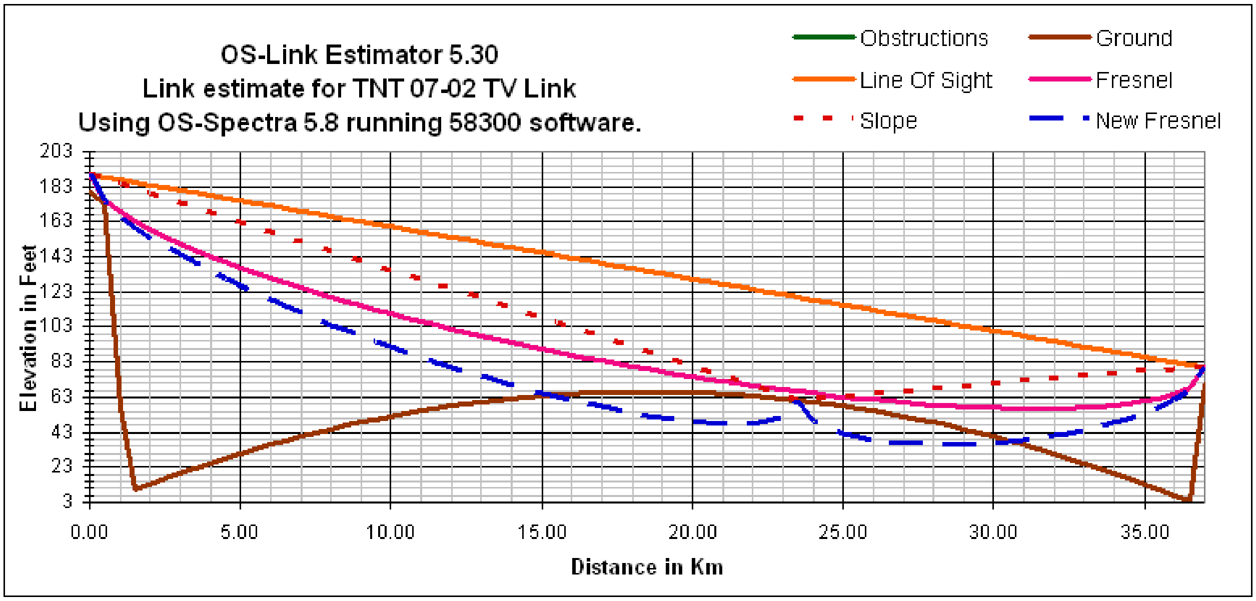


Figure 43 TNT 07-02 MIO Maximum Predicted Link Distance.

F. PHASE III EXPERIMENT – OPERATIONAL IMPLEMENTATION IN SUPPORT OF EXERCISE TALISMAN SABER 2007

Exercise TALISMAN SABER is a bi-annual U.S. Pacific Command-sponsored exercise designed to train the U.S. Seventh Fleet commander's staff and Australian joint operations staff as a designated joint task force (JTF) headquarters. The exercise focuses on crisis action planning and execution of contingency response operations. U.S. Pacific command units and Australian forces conduct land, sea and air training throughout the training area. In 2007 the TALISMAN SABER was conducted at the Australian Defense Force (ADF) Shoal Water Bay Training Area (SWBTA) 60 km north of Rockhampton, Queensland in Australia. Over 30,000 U.S. and Australian forces representing each of the four services of each country participated in the exercise.

Naval Postgraduate School was invited to participate in the exercise by Commander, Seventh Fleet (C7F) Code N39. As part of the exercise, NPS personnel would participate in the Science and Technology (S&T) field experiments sponsored by Commander, Pacific Command (PACOM) Code J85. Naval Postgraduate School personnel would establish an autonomous communications network independent of operational networks in order to facilitate experimentation efforts by Naval Research Laboratory (NRL), Naval Information Operations Command (NIOC), Suitland, Maryland, and Air Force Research Laboratory (AFRL), Wright-Patterson Air Force Base, Dayton, Ohio. Each serviced organization would use the data communications network established by NPS to transmit experiential data and unclassified operational data in support of their respective operational sponsors.

Figure 44 shows the overall topology that was implemented by NPS during TS 07. The total terrestrial distance covered by the network was over 60 km spanning from 10 nm off of the coast to 35 km inland.

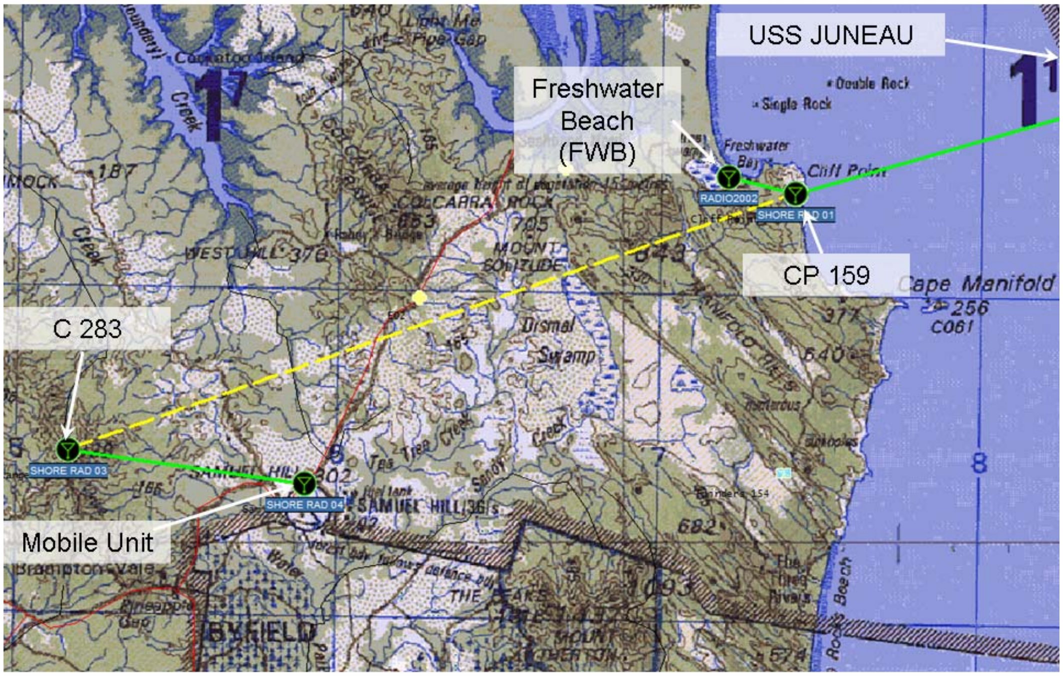


Figure 44 TS 07 NPS Network Topology.

1. Exercise Scenario

NOTE: Due to the sensitive nature of military operations, tactics, and procedures, only general, unclassified descriptions of events, scenarios, and tactics which took place during Exercise TALISMAN SABER 07 will be provided in this section.

The operational scenario for TALISMAN SABER 07 (TS 07) was the response of U.S. and Australia forces to rising political tension between two neighboring fictional countries. As the political crises continued to grow, U.S. and Australian forces would develop response plans for diffusing the crises between the two countries up to, and including, plans for military action against the aggressor country. When the aggressor nation invaded its neighbor, coalition forces would begin military operations to stop the aggressor nation, drive them out of the invaded territory and return political stability to the region. Coalition military actions would include a combination of tactical air strikes and amphibious landings in the vicinity of the occupying forces. The network installed by NPS in support of the exercise would be used to help facilitate experimentation conducted during the exercise.

2. General Network Topology

As previously stated, the NPS installed wireless network employed during TS 07 was an autonomous network completely independent of any existing military operational network. This independence allowed NPS to quickly modify network topology on both the shore and at sea as scenario and operations required without having to seek official network accreditation or re-accreditation as network function and topology changed. Additionally, it allowed those organizations being serviced by the NPS TS 07 network to conduct experiments that would normally require high level authorization if conducted on an operational military communications network.

The NPS network was comprised of a combination of one set of Motorola PTP 400, two sets of Motorola PTP 600, and one set of Redline AN-80i 802.16 wireless point-to-point (PtP) radios. In order to facilitate non-line of sight (NLOS) and multiple line of sight (LOS) shots called for in the topology shown in Figure 44, relay sites were constructed to allow multiple PtP links to terminate at a single location yet still be part of the overall data network. The relay sites were constructed by connecting the Ethernet ports of the radios terminating at the site into a 24-port 1000 Mbps switch at the site allowing the simulation of a point-to-multi-point (PtMP) data link using only PtP radios. All of the IEEE 802.16 based radios used in the NPS radio-WAN operated in the 5.8 GHz unlicensed UNII frequency band.

a. Node Sites

(1) Cliff Point 159 (CP159). Cliff Point 159 was located on the eastern boundary of SWBTA in the vicinity of Freshwater Beach. This site was at an elevation of 159 meters (521 ft) above mean sea level (AMSL) and consisted of grassy vegetation with an average height of approximately 1 m (3.28 ft) and rocky soil. This site was chosen due to its accessibility, proximity to the Coral Sea, proximity to Freshwater Beach, and LOS to C 283 (described below.) There were no facilities at the site and

power was provided by an 800 W gasoline generator which required daily trips to the site to refuel and maintain the generator. Access to the site was by an untended foot trail from the beach front to the peak of the feature. Cliff Point 159 acted as a relay node for the USS JUNEAU-CP 159, FWB-CP 159, and C 283-CP 159 data links.

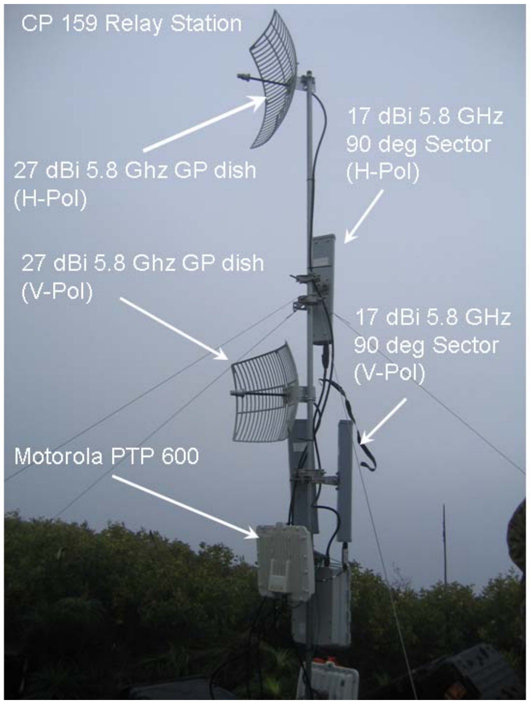

CP 159 Relay Station
27 dBi 5.8 Ghz GP dish (H-Pol)
17 dBi 5.8 GHz 90 deg Sector (H-Pol)
27 dBi 5.8 Ghz GP dish (V-Pol)
17 dBi 5.8 GHz 90 deg Sector (V-Pol)
Motorola PTP 600

Figure 45 Cliff Point 159 Relay Station.

To construct the site, three (3) 5 foot lengths of galvanized steel piping were connected by threaded couplers to form a 15 foot tall mast. The mast was placed into a stone footing at the site and stabilizing with four (4) 8 foot wire strand guying wires.

The JUN-CP159 link was constructed by placing two horizontally polarized and two vertically polarized 90 degree 5.8 GHz sector antennas at the top of the site mast. The vertically polarized antennas were placed at the top of the mast and the horizontally polarized antennas were placed three feet below the bottom of the vertically polarized antennas. Motorola PTP 600 radios were used to create the radio-WAN data link. In order to lower the center of gravity of the antenna mast and help stabilize the mast, the radio was mounted at the bottom of the mast approximately 2 feet from the ground. Ten foot lengths of LMR 400 coaxial RF cabling was used to connect the horizontal and vertical RF feeds on the radio to the respective antennas. In order to provide RF feed to two antennas per polarized feed, a 4-way RF splitter was installed before the antennas. One of the antennas was then set at an azimuth of 045 and the other set to 135 allowing for 180 degrees of coverage from 000 to 180. The same method was used to install the horizontally polarized antennas. This site would act as the base station (BS) for the JUN-CP159 data link.

The FWB-CP159 link was constructed by using Redline AN-80i 802.16 wireless radios with integrated 1 foot, 22 dBi 5.8 GHz antennas. One of the AN-80i radios was mounted immediately below the horizontally polarized antenna array used for the JUN-CP159 data link. The radio was set to an azimuth of 285 and the elevation visually adjusted to service FWB. The radio was then configured to act as the BS for the data link.

The C 283-CP159 link was comprised of Motorola PTP 600 5.8 GHz radios and 27 dBi 5.8GHz grid-parabolic dish antennas with a vertical and horizontal beam with of 6.5 degrees. One antenna was mounted on the mast in a vertically polarized configuration, the other antenna was mounted on the mast in a horizontally polarized configuration. As with the USS JUNEAU-CP 159 radio, the 802.16 radio was mounted low on the mast to lower the center of gravity of the mast thus increase stability. The radio was connected to the antennas using two (2) 10 foot lengths of LMR 400 coaxial RF cable and then set to an azimuth of 255 (the magnetic heading to C 283.)

All three radios were connected to a base kit for power and IP connectivity. The base kit was a pre-constructed kit consisting of:

- 1 – 1U 24-port gigabyte switch
- 1 – 15A 6 outlet power strip
- 2 – Motorola POE injectors
- 1 – Redline POE injector

Due to the location of CP159 and the difficulties of accessing the site, CP 159 was only operated during the day due to safety concerns. The generator was capable of powering the site for approximately eight (8) hours unattended. While only providing eight hours a day of link operation, this amount of time was sufficient for the purposes of those being serviced by the data links.

(2) Freshwater Beach (FWB). Freshwater Beach is located on the eastern boundary of SWBTA and provides a protected harbor from the Coral Sea. This site was the primary landing site for U.S. and Australian amphibious forces throughout the exercise. As seen in Figure 46, the site was characterized by dense vegetation leading up the shore line and approximately 50m (174 ft) of beach area. A hard packed dirt road provided the only access to the site. No power was available at the site.

The SS for the FWB link was comprised of a Redline AN-80i which matched the one installed at CP159. The unit was mounted on a 10 foot temporary mast which was tethered to a rental Landrover operated by NPS. A single laptop connected directly into the Redline POE injector was used for data communications at the site. Power was provided at the site by connecting an 1100 W AC/DC inverter to the battery of the mobile unit at the site.

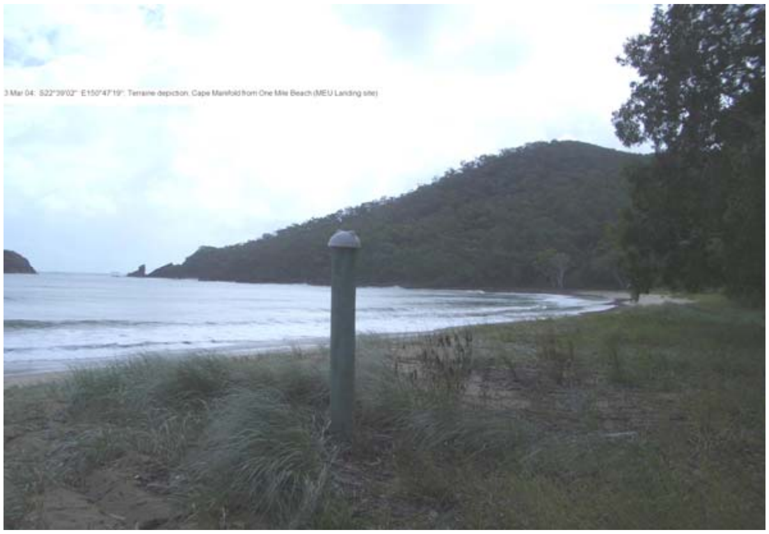

3 Mar 04: S22°39'02" E150°47'19": Terraine depiction: Cape Manifold from One Mile Beach (MEU Landing site)

Figure 46 Freshwater Beach (FWB) Amphibious Landing Zone.

(3) Cliff Range 283 Feature (C283). The C283 site was located approximately 35 km inland from CP159. Access to the feature was by a narrow ridgeline vehicle trail which passed through 11 km of densely forested territory. The site was located in a small clearing at the top of the terrain feature at an elevation of 283m (928 ft) AMSL as measured by GPS. This site was also occupied by a White Force (neutral team) Signal Intelligence (SIGINT) detachment from the Royal Australian Air Force (RAAF). After discussions with the Non-Commissioned Officer in Charge (NCOIC) of the detachment, NPS was allowed to use a portion of their camp for installation of the NPS radio-WAN relay station. Additionally, permission was granted for NPS to tie into the detachment's portable generator to power the radio-WAN relay station. The RAAF detachment manned the site continuously.

Cliff Range 283 acted as a relay node for the C283-CP159 and C283-MU data links. To construct this site, two (2) 5 foot lengths of galvanized steel piping were connected by threaded couplers to form a 10 foot tall mast. The mast was placed into a stone footing at the site and stabilizing with four (4) 8 foot wire strand guying wires.

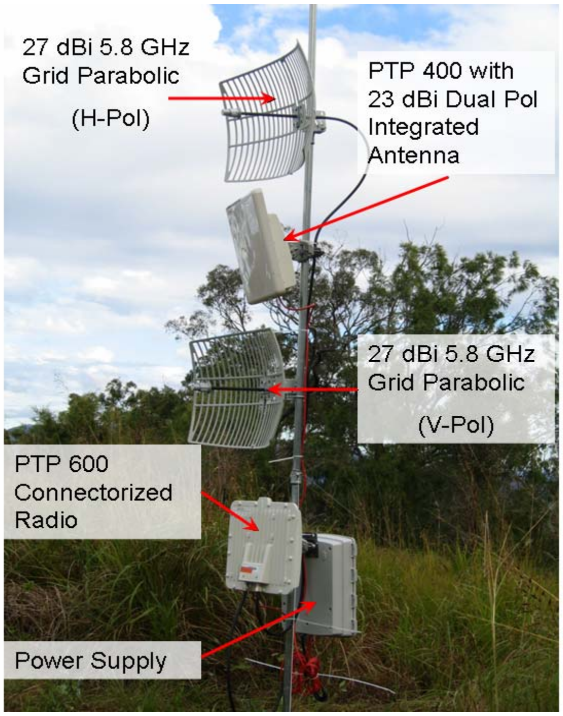


Figure 47 Cliff Range 283 (C 283) Relay Station.

The CP159- C283 link was comprised of Motorola PTP 600 radios and 27 dBi 5.8GHz grid-parabolic dish antennas with a vertical and horizontal beam with of 6.5 degrees. One antenna was mounted on the mast in a vertically polarized configuration; the other antenna was mounted on the mast in a horizontally polarized configuration. The Motorola PTP 600 radio was mounted low on the mast in order to lower the center of gravity of the mast thus increasing stability. The radio was connected to the antennas using two (2) 10 foot lengths of LMR 400 coaxial RF cable and then set to an azimuth of 075 (the magnetic heading to CP 159.)

The C 283-MU link was comprised of Motorola PTP 400 radios. The BS radio was installed at C283 and was a variant of the radio system that included a dual-polarized integrated 27 dBi antenna. The radio was installed below the grid-parabolic dishes installed for the CP159- C283 data link.

Both radios were connected to a base kit for power and IP connectivity. The base kit was a pre-constructed kit consisting of:

- 1 – 1U 24-port gigabyte switch
- 1 – 15A 6 outlet power strip
- 2 – Motorola POE injectors
- 1 – Redline POE injector

(4) NPS Mobile Unit (MU). The NPS Mobile Unit was located at various locations throughout the exercise. The primary area of operations was a stretch of roadway located approximately 10 km SSE of C283. This area was heavily forested, relatively flat with respect to terrain features and located at an average of 50m (164 ft) AMSL. The MU consisted of a Motorola PTP 400 radio with external antennas mounted on a Nissan Patrol 4-wheel drive rental vehicle. Power to the radio was provided by connecting the vehicle’s battery to an 1100 W AC/DC inverter.

(5) USS JUNEAU [LPD 10] (JUN). The sea based portion of the NPS radio-WAN network was installed on board the USS JUNEAU (LPD 10.) NPS was allowed to install the SS above the Signal Shack on the O4 level, forward of the

vessel's main mast and aft of the WSC-6 radome. At approximately 85 feet above the ship's waterline, the site provided a good height of eye for the radio-WAN node on the USS JUNEAU. However, RF blockage was experienced forward and aft of the site due to the WSC-6 radome (forward) and the ship's main mast (aft.) The forward blockage caused by the WSC-6 radome spanned from 300 to 060 relative. The aft blockage caused by the main mast spanned approximately 135 to 225 relative. These blockages left a usable RF coverage area of 060 – 135 on the starboard side of the vessel and 225 – 300 on the port side; 75 degrees of coverage on either side of the ship. Though only 75 degrees of coverage was possible on the port and starboard side of the ship, respectively, this coverage was adequate for the purposes of establishing and maintaining a data link with CP159.

A more optimal installation site would have been the O6 platform on the main mast. However, installation on this platform would have required securing critical shipboard communication system during the installation process; this was not possible during the period of time in question.

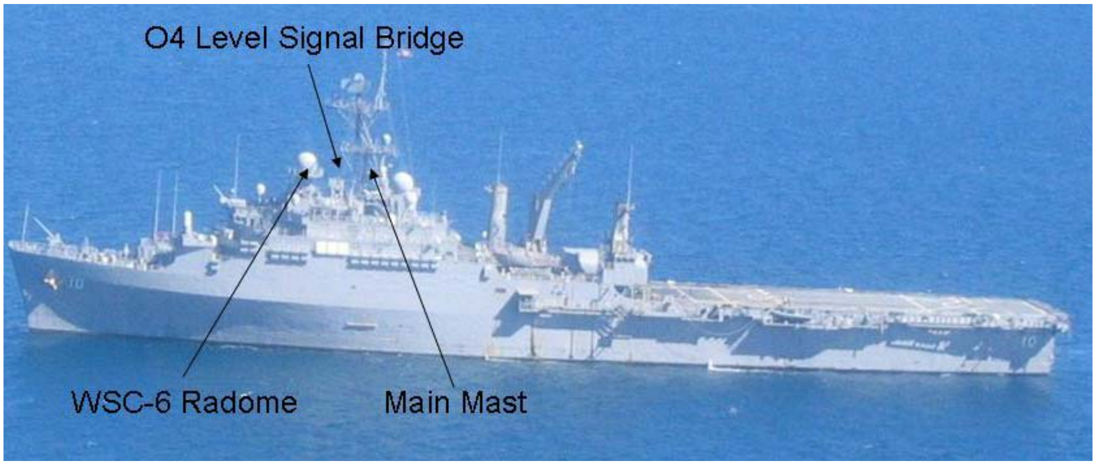


Figure 48 USS JUNEAU Site Location.

During the period of June 28-30 the USS JUNEAU was ordered by their ESG Commander to act as beach guard for the FWB amphibious LZ. Their operational boundaries were restricted to a northern limit 5 nm north of FWB, a southern limit of 5 nm south of FWB, and a distance of 8 – 10 nm from FWB. This narrow OPAREA restricted the USS JUNEAU to courses of 000 or 180 except when other courses were required in order to support flight or LCAC operations. Due to this limited operational area, NPS was able to maintain continuous communication with CP159 in all portions of the USS JUNEAU OPAREA with the 75 degrees of coverage provided on either side of the ship. The only time that data links were lost was when the ship reached the northern or southern limit of their OPAREA and turned around to steam to the opposite boundary. As the ship turned and passed through headings which included the shadow zones caused by the WSC-6 radome and main mast, the link to CP159 was disrupted and the link was lost. When the ship steadied onto its new course of 000 or 180, the link was re-established.

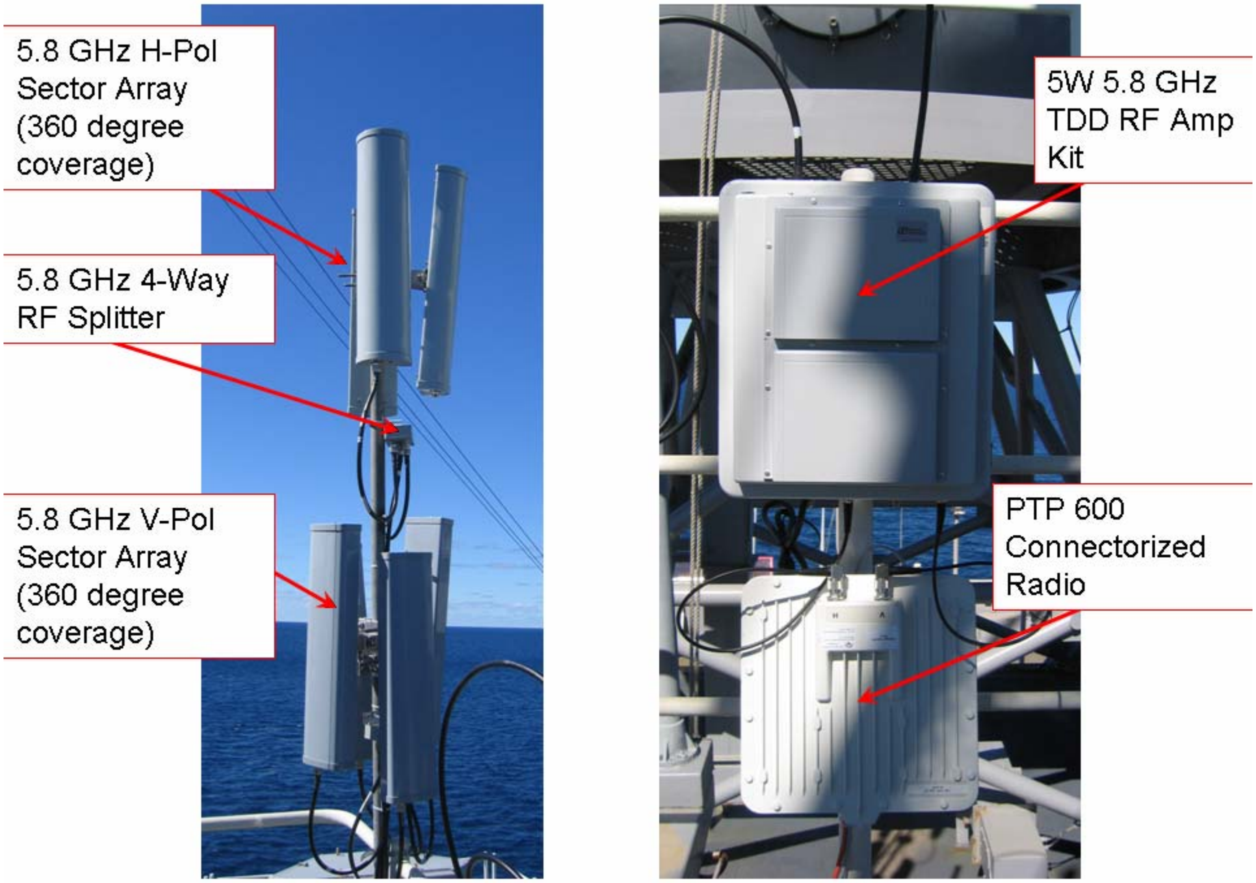

5.8 GHz H-Pol Sector Array (360 degree coverage)
5.8 GHz 4-Way RF Splitter
5.8 GHz V-Pol Sector Array (360 degree coverage)
5W 5.8 GHz TDD RF Amp Kit
PTP 600 Connectorized Radio

Figure 49 USS JUNEAU Subscriber Station.

The SS site installed on the USS JUNEAU was comprised of a Motorola PTP 600 radio, 5 watt 5.8 GHz RF amplifier kit, 4-element horizontally polarized 5.8 GHz antenna array, and a 4-element vertically polarized array. A 10 foot 2” diameter mast was temporarily installed on the O4 Signal Shack by the NPS team with the assistance of the E-Division CPO. The vertically polarized antenna array was installed at the top of the temporary mast and the array elements set to relative bearings (referenced to the ship) of 000, 090, 180, and 270 to provide 360 degrees of coverage; the elevation of each element was set to +4 degrees from a horizontal plane. The horizontally polarized array was installed 3 feet below the vertically polarized array and set to the same relative bearings; the elevation of the elements was set to -4 degrees from horizontal. By setting the elevations of the antennas to +4 and -4 degrees from horizontal the total horizontal coverage offered by the array was extended to 16 degrees allowing for a greater tolerance range of pitch, roll and yaw cause by wave action on the USS JUNEAU.

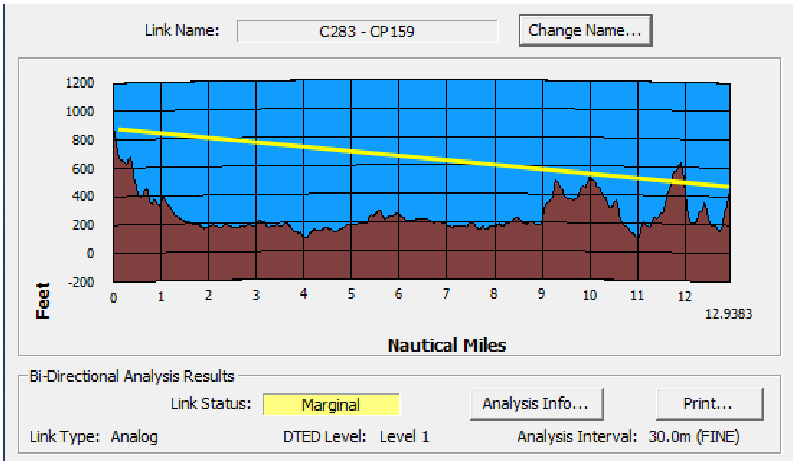
The 5 W amplifier kit was mounted at the base of the mast on a permanent stanchion on the platform. The Motorola PTP 600 radio was mounted immediately below the amplifier kit on the same stanchion. The vertical and horizontal radio inputs were connected to the amplifier kit with 2 – 2 foot LMR 200 coaxial RF cables. Two 10 foot LMR 400 coaxial RF cables were used to connect the amplifier kit to the 4-way RF splitters used by the horizontal and vertical antenna arrays. From the 4-way RF splitters to each antenna 2 foot LMR 200 coaxial cables were used. Power for the system was provided by ship’s 60 Hz power.

3. Results

From 25 – 30 NPS personnel on board the USS JUNEAU conducted various communication experiments supporting NRL, Combat Camera, and NIOC Suitland. Initial NPS specific shore-based test results were as follows:

C 283 – MU:	21 Mbps at 8.5 km
CP 159 – C 283:	55 Mbps at 37 km
CP 159 – FWB:	54 Mbps at 2.1 km

On 25 June, the C283–MU data link began experiencing RF interference from an unknown source. The interference was seen only at the MU SS. All attempts to adjust the operational frequency of the SS and BS failed and the link was secured on the advice of TS 07 exercise control (EXCON) to ensure that the link was not interfering with operational communications necessary for the exercise.



Link Name: C283 - CP159

Bi-Directional Analysis Results

Link Status: Marginal

Link Type: Analog DTED Level: Level 1 Analysis Interval: 30.0m (FINE)

Figure 50 CP159 to C283 Link Profile.

a. NRL NOVISS Testing

On 26 June NPS conducted short range operational tests in conjunction with NRL and COMCAM in support of NOVISS video testing. Original test plans called for the use of the NPS radio-WAN to carry live streaming video from a mobile site 10 km south of C283 to FWB. However, due to the local RF interference with the C283–MU data link, ad hoc test plans were developed to facilitate NRL test requirements. Spare Motorola PTP 600 radios were temporarily installed at a military vehicle wash-down site and set as the BS for the link. The Motorola PTP 400 radio that was installed on the Nissan Patrol was replaced with a Motorola PTP 600 radio; the 90 degree sector antennas installed for the PTP 400 system were used for the PTP 600 system.

The MU was driven to a distance of 2 km from the BS. As the test commenced, COMCAM began recording video of the event. The MU was driven towards the BS at a speed of 15 kph. At 1.2 km a stable link was established with the BS through dense foliage in NLOS conditions. Observers at the BS were able to view high quality video transmitted form the MU while the MU was in motion. The test was repeated several times with the same results. The average SNMP report throughput was 14.4 Mbps; no *IXC* testing was performed on the link.

While 1.2 km is a relatively short distance, especially when compared to the 200 km maximum distance rating of the Motorola PTP 600 radios, the link was established through dense vegetation in NLOS conditions over hilly terrain. Previous testing by NRL in the same location in identical conditions using 802.11g based WLAN equipment yielded a maximum distance of 300 yd in LOS conditions and 110 yd in NLOS conditions.

b. NPS Ship-Shore 802.16 Data Link Testing

Testing of the CP159-JUN data link was conducted on 29 and 30 June in conjunction with other experimentation efforts. Due to operational tasking, the USS JUNEAU was limited to a speed of 7 kt throughout the testing window. Sea state during both days of testing was virtually 0; seas and winds were calm leading minimal pitch, roll, and yaw of the ship. Both *SolarWinds* and *IXC* were used to measure the parameters of the CP159-JUN data link.

During the test series the USS JUNEAU was restricted to a narrow operational area 8 – 10 nm to support actual military operations, as such the original NPS test series which called for link distances from 1 to 20 nm was not approved by the ESG commander. A new test series was drafted and submitted which enabled testing during the USS JUNEAU patrols and did not interfere with USS JUNEAU operational duties. While not allowing for maximum distance testing, the test series would allow for proof-of-concept testing of an at-sea IEEE 802.16 based radio-WAN communication system.

During both days of testing, the CP159 site was manned by shore-based NPS personnel. The USS JUNEAU was manned by NPS personnel who were transported to the USS JUNEAU by USMC CH-46 helicopter prior to the beginning of the test series.

Figure 51 shows a summary of SNMP reported link performance over a one and one quarter (1.25) hour test period. During this period USS JUNEAU was operating at approximately 9 nm from shore at a speed of 7 kt. From time 19:18 to 19:20 the link is shown to vary from an rxSig of -65 to -69 dBm. From time 19:20 to 19:35 the rxSig becomes more erratic; this was due to the ship slowing and turning to a course of 080 for LCAC recovery operations. During this time the main mast of the ship was directly in the LOS between CP159 and the array on the USS JUNEAU. When the ship resumed its original course at 19:35, unobstructed LOS to CP159 was regained and rxSig stabilized. This phenomena was seen throughout the testing period when USS JUNEAU performed LCAC and helicopter operations. Due to the position of the 802.16 array on the USS JUNEAU, these link interruptions were unavoidable.

During the periods of normal operations, the CP159-JUN data link remained very stable with rxSig variations of less than 10 dBm. On Day 1, SNMP reported throughput ranged from 12.5 Mbps to 30 Mbps. Testing conducted with *IXC* show a usable throughput of 21 Mbps (average) with a latency of less than 10 ms. Similar results were shown during Day 2 of testing. During Day 2, maximum SNMP reported throughputs of 37 Mbps with a corresponding usable throughput of 29. 5 Mbps as recorded by *IXC*. Table 3 summarizes the results obtained through *IXC* testing on both days testing was performed. As can be seen from the results, median throughput for both days of testing is over 20 Mbps with minimal jitter and latency. Median data transferred during the test runs was over 165 MB of TCP, UDP, and RTP traffic over a one minute test period.

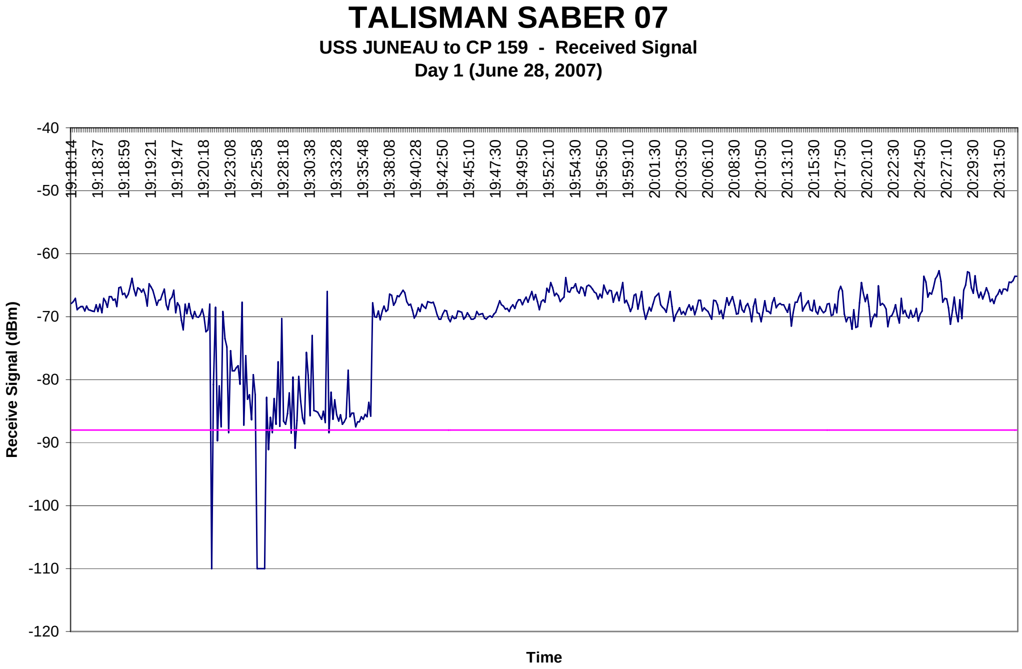


Figure 51 TS 07 Ship-Shore Data Link Received Power.

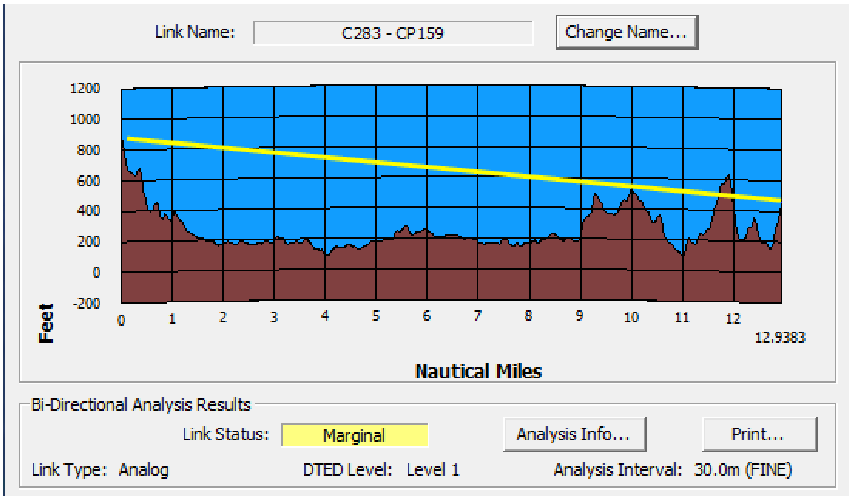
TS 07 JUN - CP 159 IX Chariot Results								
		VOIP MOPs				Data Amounts Tx/Rx		
Throughput (MBps)	Latency (sec)	MOS	Delay (ms)	Lost Data (%)	Jitter (ms)	MB Sent (MB)	MB Received (MB)	Total Data (MB)
13.668	3.035	3.82	12	0.28	1.184	104.107	0.800	104.907
9.794	4.014	4.34	27	0	0.912	74.115	0.823	74.938
21.607	2.022	4.32	14	0	0.775	164.223	1.142	165.365
24.199	1.802	4.37	3	0	0.412	184.229	1.159	185.388
21.610	2.014	4.37	9	0	0.612	164.227	1.153	165.380
21.100	2.023	4.29	16	0	0.625	164.215	1.119	165.334
21.617	2.017	4.34	10	0	0.600	164.225	1.148	165.373
29.465	1.479	3.22	7	0	0.475	224.240	1.194	225.434
12.421	3.136	4.30	21	0	0.712	94.136	0.887	95.023
17.626	2.362	3.89	12	0.17	0.592	134.172	0.991	135.163

Table 3 TS 07 CP159 - JUN IX Chariot Summary.

4. Test Conclusions

The NPS network constructed during the exercise successfully demonstrated the use of IEEE 802.16 wireless networks in a tactical environment under realistic battle field conditions. The efficiency with which the shore-based links were installed, configured, and brought online highlights the potential IEEE 802.16 based radios, such as the ones employed during TS 07, hold for U.S. and coalition forces in battle fields in the future.

The results achieved by the shore-based links were not unexpected. Prior experience by the author with constructing IEEE 802.16 radio-WANs has shown that data links of this nature can work in a variety of environments and scenarios which closely mimic those of battle field conditions. However, the CP159-C283 did prove a surprise. The original site planning for the relay sites showed an unobstructed line of sight between CP159 and C283. Once the team arrived on site for an initial survey of the previously selected sites, it was discovered that the mapping data for the area was inaccurate and a significant terrain feature obstructed the line of sight. Despite reservations, the link was constructed and brought online with the hope that diffraction would allow the link to establish; it did. Even with a 35m (115 ft) obstruction in the link, the link came online and operated at a stable 55 Mbps.



Link Name: C283 - CP159

Bi-Directional Analysis Results

Link Status: Marginal

Link Type: Analog

DTED Level: Level 1

Analysis Interval: 30.0m (FINE)

Figure 52 CP159 to C283 Link Profile.

The ship-to-shore data link did not perform as planned. The link calculations performed prior to arrival on site indicated that at least 120 Mbps would be available on the data link. As the results show the data link averaged 21 Mbps. This represents a significant disparity between predicted and actual results. After troubleshooting the data link extensively and consulting with the manufacturer, the only plausible explanation is the reflective interference caused by the position of the site on board the USS JUNEAU. The obstructions caused by the WSC-6 radome forward of the array and the main mast aft of the array may have acted as reflective surfaces for the signals being transmitted and received by the SS. These reflections would show up as multi-pathing in the RF environment reducing the efficiency of the radio as it was forced to continually adjust modulation and power to correct for the multi-pathing. This theory is supported by the increase in throughput seen on the second day of testing when the forward and aft elements of the array were taken offline leaving only the port and starboard arrays to transmit and receive.

The ship-to-shore data results, while not as predicted, do represent a significant improvement over current ship-to-shore terrestrial wireless communications in use by the U.S. Navy and Marine Corps. Currently the only comparable system for wireless data communications between ships or to the shore is the Direct Wideband Transmission System (DWTS.) This system is currently designed for a maximum throughput of 2.048 Mbps under optimal conditions. After speaking various members of the Communications Department staff on the USS JUNEAU, the maximum throughput they have been able to achieve with DWTS is 512 kbps at 4000 yds.

G. SUMMARY

Throughout the series of field experiments conducted in support of this thesis, throughputs and link stability are shown to continually increase as installation and operational procedures were continuously honed, enabling the development of a prototype system capable of being fielded in an operational military environment. When compared to single radio performance, the MIMO technology used by Motorola PTP systems shows significant performance advantages that cannot be ignored. As seen when comparing the Redline AN-50 system to the Motorola PTP 600 system in similar at sea conditions, the stability of the rxSig is dramatically higher for the PTP 600 system illustrating the performance gain achieved when using a MIMO approach to establishing wireless long-distance terrestrial communications in a dynamic environment. While this in no way flat endorsement of MIMO technology in all environments, it does show that MIMO technology offers significant performance increases in dynamic environments that are present over open water with mobile platforms and constantly changing propagation paths.

Test results also show that current IEEE 802.16 WLAN radios perform well in some of the demanding environments that the military operates in. These tests show that with simple modifications to commercially available materials, a viable wireless communications system can be developed which functions better than program-of-record systems currently in use by the U.S. Navy and Marine Corps. With further study and development, military grade systems can be developed that can meet the most demanding environments while maintaining high performance and meeting the current and future communications needs of the military.

THIS PAGE INTENTIONALLY LEFT BLANK

V. NECESSARY IMPROVEMENTS

A. DISCUSSION

The results of the experimentation discussed in the previous chapter illustrate the efficacy of IEEE 802.16 based wireless communications in tactical network environments both at sea and on the shore. Using commercially available equipment, communication systems were developed and implemented in a variety of physical environments to demonstrate the capabilities and characteristics of systems and the potential benefits to military communication networks. Despite the potential shown by the IEEE 802.16 based radios used for this research endeavor, more work is needed prior to wide spread deployment of IEEE 802.16 based communications in the military.

Current iterations of IEEE 802.16 based wireless communications were designed and developed for commercial communications systems. While these communication systems share the same quality of service requirements that are needed for a military communication system, they do not share the high level of security requirements, nor do they share the same requirements for system mobility or dynamic topology. This is not due to a failure or immaturity of the technology; it is due to a lack of focused market demand in the commercial and military sectors. The manufactures have designed and built communication systems based on their customers needs.

The areas for improvement discussed below represent a suggested list for further research and design based on the results of this and previous thesis research efforts. The areas focus on both the IEEE 802.16 protocols and supporting technologies that must be addressed in order to develop an overall system capable of meeting the current and future communications needs of the U.S. Navy and Marine Corps while seamlessly complementing other communication systems employed by the militaries of both the U.S. and coalition partners.

B. TECHNICAL AREAS

1. Antenna Technology

While not specifically part of IEEE 802.16 based technology, antennas are a supporting technology that must be addressed. As with any wireless communications system, the antenna is a critic component without which the wireless system is rendered inoperable, or severely reduced in capability. Wireless communications based on IEEE 802.16 technologies are no different than other wireless communications systems; the operation of the radio is a function of the antenna. As such, an advance in antenna technology is the most critical factor in developing and implementing an effective tactical radio-WAN network in an intra battle group scenario.

Most current utilization of IEEE 802.16 based wireless communications in both the civilian and military sectors is in static, non-mobile PtP communication links. Since the base and subscriber stations do not move, high gain antennas having very narrow vertical and horizontal beams can be used to maximize the performance of the links. Current commercially available antenna designs work exceptionally well in these types of environments. However, when the platform mobility and ad hoc networking inherent in a tactical network design are taken into consideration, these antenna designs prove to be inadequate.

Currently the only alternatives to high gain directional antenna systems are Omni-directional and sector antennas. While giving a wider horizontal and vertical beam width than directional antennas, these variants have a lower passive gain. However, the wider horizontal beam width offered by these types of antennas do allow the “aiming slack” required to maintain connectivity between two IEEE 802.16 based radio-WAN nodes while their associated platforms are in motion. Unfortunately the reduced gain of these antennas decreases the link ranges that can be achieved by these radios.

In order to achieve the high gain of directional antennas and the wide coverage of Omni-directional and sector antennas, steerable, or switched beam antennas must be developed. Steerable antenna systems would allow for (Olsen):

1. Higher Passive Gain – a higher passive gain would enable longer link distances and better link performance overall.

2. Higher Data Rates – with both radios using antennas that are constantly in optimum alignment, the received signal (rxSig) for both antennas will always be maximized. With rxSig continuously at maximum levels, the modulation of both radios can be maximized resulting in greater data rates over the wireless links.

3. Reduced Electromagnetic Signatures – reducing the electromagnetic (EM) signature of a military unit is, and will continue to be, a major concern with respect to detection by opposing forces. The greater the EM signature of a military unit, the higher the probability will be of detection and geolocation by enemy units. By using a tightly formed beam for IEEE 802.16 based communications, the overall EM signature of the unit is reduced while still enabling high bandwidth and reliable wireless communications.

4. Greater resistance to jamming – the use of tightly formed RF beams to establish IEEE 802.16 radio-WAN data links would require any adversary attempting to actively jam the RF signal to locate their transmitter directly in the RF beam. RF jamming outside of the friendly beam would stand a low probability of interference with friendly communications.

5. Rapid system deployment in field environments – The most time consuming portion of establishing long distance IEEE 802.16 based radio-WAN communication links is the aiming of antennas on the base and subscriber stations. While aiming antennas becomes a mute point using sector or Omni-directional antennas, these antennas will be lower gain, have a much larger EM signature, and are in general an inefficient use of RF energy. In tactical scenarios communication units rarely have the luxury of time. With that in mind nodes must be capable of being established in a short period of time with minimal effort.

a. Phased Array Antenna Systems

Phased array antenna systems are currently in use many military systems such as the SPY-1 RADAR system employed by AEGIS destroyers and cruisers. The array allows multiple individual RF beams to act as a single unit enabling a highly accurate means for transmitting RADAR energy. However, the system has two primary draw backs with respect to data communications: 1) it is extremely large and non-portable, 2) it is very expensive (Olsen). While a phased array system would be the "ultimate" antenna system for an IEEE 802.16 based tactical network, the cost and size would restrict its use to a limited number of platforms and deployable forces.

b. Steerable/Switched Beam Antenna Systems

These types of antenna systems hold two significant advantages over phased array systems: 1) cost and 2) size. While performing the same basic function of a phased array antenna system, switched beam antenna systems, by design, are theoretically much smaller and cheaper than phased array systems.

Dr. Randell Olsen (Code 80) at SPAWAR Systems Center, San Diego is currently leading a team of RF engineers whose goal is to design a low cost steerable/switched beam antenna array with a unit cost of less than $1,000 (Olsen). Such an antenna design is a critical factor in enabling wide-scale use of IEEE 802.16 based radio-WAN communications in tactical scenarios.

c. Self-aligning Antenna Systems

Self-aligning antenna systems are another variety of "smart" antennas. In the case of self-aligning antenna systems a directional or sector antenna is mounted on a mechanical pan-tilt-zoom (PTZ) platform. Control signals are sent on a sub-frequency that allows the system to maximize the rxSig through continuous aiming of the attached antenna. While the construction and design of a self-aligning antenna system is simple and relatively inexpensive, these types of antenna systems are useful for PtP data links only. In order to create PtMP or fully meshed topology, potentially dozens of self-aligning antenna systems would be required creating a mechanically complex system which few platforms could host.

2. Multiple Access Systems

In tactical scenarios, both at sea and on land, military units must be able to communicate with each other without relying on a single communications relay point; a single relay point leaves all of the units open to a single-point failure of communications. For redundancy and reliability, a fully meshed communications network is required. In the event one node fails, the impact on other nodes is minimal.

Currently, several vendors offer point-to-multipoint IEEE 802.16 based wireless radios which allow multiple subscribers stations to connect to single base station creating a hub and spoke wireless network; similar in design to a controlled radio network having a network control station (NECOS.) However, if that base station fails, the entire wireless network will collapse.

A more reliable and flexible solution is a fully meshed tactical network. In this network architecture no single station would act as a controlling unit; radios would connect to the nearest available node. The redundancy and flexibility of an IEEE 802.16 based meshed tactical network would offer tactical units the communications assurance required in tactical scenarios and allow the flexibility in network topology required to adapt to the ad hoc nature of tactical networking.

The IEEE Std 802.16-2005 addresses standards required to incorporate system mobility into IEEE 802.16 based radio-WAN. With the adoption of the 2006 standard, commercial ventures were quickly launched develop mobile IEEE 802.16 based radios for use in laptops, etc. While development is on going, commercially available systems are expected to be offered by manufacturers such as Intel, Fujitsu, and Toshiba in the very near future.

3. Frequency Variants

The IEEE 802.16 protocol standard covers radios which operation over a frequency range of 2 to 60 GHz. It important to note that the MAC layer protocol specifications of the IEEE 802.16 standards are the same regardless of the frequency range the radio is designed to operate in. Most commercially available IEEE 802.16 based radios operate in the unlicensed 5.4 – 5.5 GHz or 5.7 – 5.8 GHz frequency bands. As the global popularity of IEEE 802.16 based wireless communications increases, both of these frequency bands will quickly become saturated with RF increasing the likelihood of RF interference or RF fratricide. Such congestion is already evident in major urban areas. In order to avoid congestion issues in urban areas in the U.S. and around the world, any IEEE 802.16 based wireless radios used by DoD should operate on frequency bands controlled by DoD (i.e., military only frequencies). In order to increase the flexibility of the radios and increase the potential for interoperability with other nations, IEEE 802.16 based radios used in tactical radio-WANs should also be able to transmit and receive signals in other frequency bands on demand. Ultimately, IEEE 802.16 based systems should be designed to operate in multiple frequency bands simultaneously.

4. Frequency Hopping

In their current form IEEE 802.16 based wireless radios are susceptible to denial of service through RF interference (aka jamming.) While the Motorola PTP 400 and 600 radios have radar avoidance capabilities enabling the radios to shift frequencies in event they detect RF interference, this capability is considered a reactive event. Proactive frequency shifting should be incorporated in order to prevent active jam attempts and to provide an additional measure of protection from passive data attacks and man-in-middle attacks.

5. X.509 Certificates

Currently only the subscriber station (SS) in IEEE 802.16 based wireless communication links are required to have x.509 certificates for authentication. The SS transmits the x.509 certificate embedded by the manufacturer in the radio to the base station which compares the certificate with an embedded hash algorithm. If authentication is successful, the BS will initiate further handshake procedures with the SS to establish the data link. This system of authentication, while much more secure than the IEEE 802.11 protocol, it leaves IEEE 802.16 based systems open to two attacks: man-in-the-middle and hijacking of the x.509 certificate of the SS.

The man-in-the-middle attack would allow an adversary to place a BS in the wireless link and take over the role of the BS; all data transmitted on the data link from that point on would be intercepted by the adversary. While the information being transmitted over the data link would not be compromised if it were encrypted with standard inline encryptors such as KG-175, KG, 84, etc, the intercepted datagrams could be manipulated causing data corruption at the receiving station.

Additionally, the x.509 certificate of the SS is embedded by the manufacturer and does not change. In the event an adversary obtains the x.509 certificate of a valid DoD IEEE 802.16 based radio, the adversary can embed the stolen x.509 certificate into another radio and establish a link with a valid U.S. BS.

In order to avoid these two vulnerabilities, any 802.16 wireless system employed in a tactical network should 1) have the ability to change x.509 certificates on a regular basis (i.e., daily crypto.), 2) require both the SS and BS to exchange x.509 certificates during the authentication process. While the other areas for study recommending in this chapter require little, if any, modification to the IEEE 802.16 protocol, this security issue could require significant changes to the security protocols of the standard.

6. Encryption

Every manufacturer of 802.16 wireless radios offers some level of encryption for data packet transmission. In the case of the Motorola 400 and 600 radios (both 5.4 and 5.8 GHz variants), Motorola offers a 128 or 256-bit AES encryption scheme for data transmitted on the radios. Redline Communications offers a 64 or a 128-bit proprietary encryption system for their radios. While both of these systems encrypt the data being transmitted over the radios, the MAC and PHY layer control messages used to control the physical parameters of the links remain unencrypted. This leaves the link open to adversaries taking control of the subsystems of the radios and creating a DOS; while the confidentiality of the data being sent over the data link may remain assured, the availability of the link may be compromised. To reduce the risk of this vulnerability, control messages should be encrypted with at least AES encryption schemes.

C. PLATFORMS

The Naval Postgraduate School has focused large amounts of research on terrestrial IEEE 802.16 based wireless communications. However, terrestrial links are, for the most part, limited to optical line of sight; the greater the distance between the nodes becomes, the higher the elevation of the nodes must be in order to maintain optical line of sight. Additionally, in the likely event that terrain features block the LOS between nodes, relay points will typically be required to get around that terrain feature. In order to overcome terrestrial-based limitations, sky-based platforms must be used.

In previous research endeavors NPS has placed IEEE 802.16 based wireless radios on a variety of lighter-than-air platforms with great success. The elevation obtained by theses platforms allowed greatly extended ranges for data links without interference from terrain features and LOS considerations. However, these platforms have three primary drawbacks in military operations:

1. Static locations – the balloons must be tethered to a fixed location. This requires personnel to establish a base camp at a predetermined location and remain there for the duration of the operation for operation and maintenance of the balloon. This removes needed personnel from other combat duties.

2. Probability of detection – Adversaries and easily see the balloon relay platform from miles away. With minimal effort, adversaries could determine the location of the balloon base station and attack it.

3. Payload Instability – unless the radio payload is tightly coupled to the balloon and the balloon is carefully stabilized, the payload will be unstable making aiming difficult and the data link unreliable.

While balloon relay stations may be viable and preferable in certain scenarios, research into placing IEEE 802.16 based wireless relay stations supporting tactical networks on more stable and reliable platforms must be undertaken. Two specific platforms that should be studied are medium to large unmanned aerial vehicles (UAV) and existing manned intelligence, surveillance, and reconnaissance (ISR) platforms already in use in the U.S. fleet, specifically E2C Hawkeye electronic platforms. Both UAV and E2C platforms would offer stable and long-term platforms enabling greatly increased distance for IEEE 802.16 based wireless communications between military units on land and at sea. Coupled with steerable beam antennas, these proposed platforms could enable IEEE 802.16 based wireless communications on the order of 400 – 500 km between link nodes.

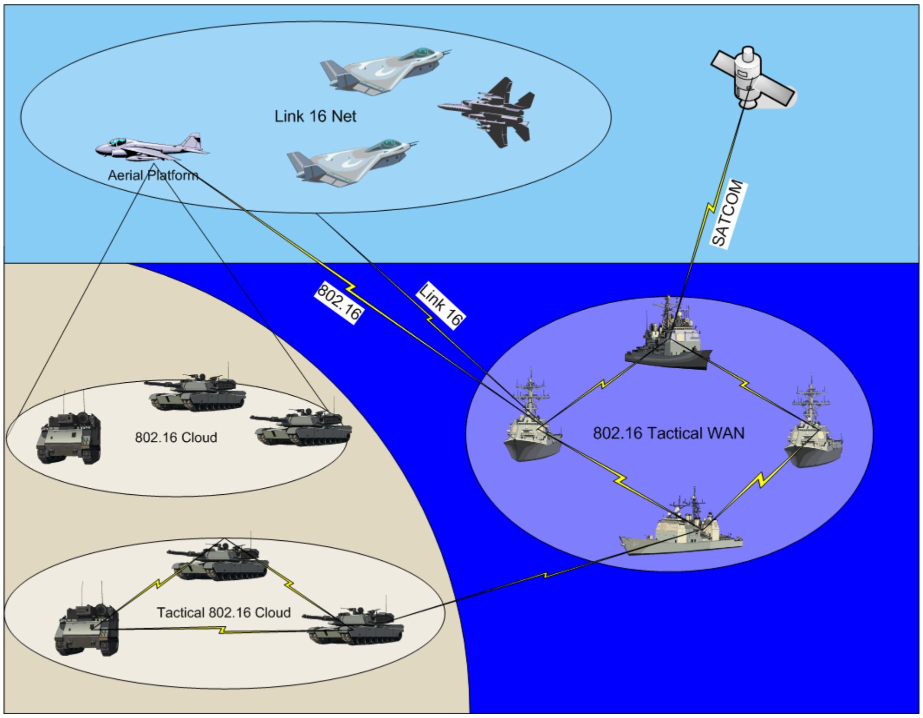


Figure 53 Basic IEEE 802.16 based Tactical Network Topology.

D. ADMINISTRATIVE

1. Routing Schemes

The tactical network architecture proposed in this thesis assumes that each major node in the tactical network is an autonomous system (AS) and that routing schemes are employed that will enable routing between network nodes having multiple data paths available to them for data transmission. Using the sample network shown in Figure 54, USS X and USS Y are AS with routers defining the boundary of their respective networks. In this scenario, if USS X must send a datagram to USS Y, the router on USS X will be able to determine the data paths available to transmit data on, determine which one is the shortest distance, and transmit the data accordingly. If the entire network shown in Figure 54 is considered a single AS, routing will become more complicated and the multiple paths available to USS X and USS Y could result in a routing loop causing routing tables contained at all of the nodes to become corrupted and cause the network to cease to function.

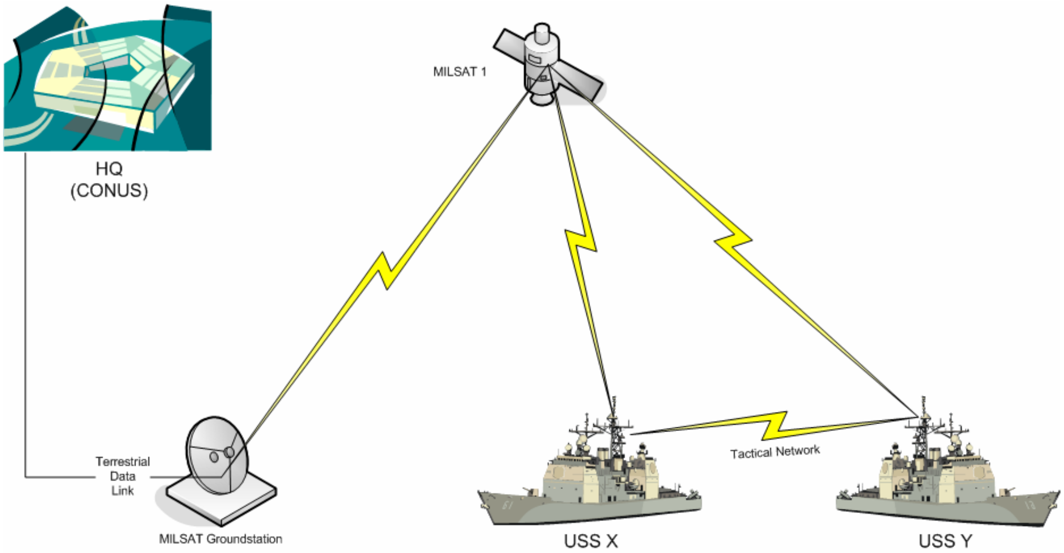


Figure 54   Basic Network.

2.   Accreditation Process

The current system for accreditation information systems is the DITSCAP. This program is required for any system that is connected to the GIG. However, no provisions have been made within the program to accredit wireless systems. As of October 2006, the ban on wireless communications on board U.S. naval vessels has been lifted, with the exception of wireless systems operating in the 3.5 GHz frequency band[19]. To date, no definite accreditation route exists for wireless data systems. As wireless data systems become more common within the DoD, joint accreditation programs must be developed that can be used for both type and site accreditation efforts.

3. Tactical Employment, Doctrine Development, and Requirements Definition

The concept of Network Centric Warfare (NCW) gives a conceptual view of an interconnected battle force capable of sharing volumes of information in an instant in order to develop and maintain an accurate and timely composite picture of the battle space; a common operational picture. While individual development efforts define the requirements for data transfer in general terms, to date there is no single document which specifically defines the amount of data that will need to be transferred by all of the systems on the network, what levels of networking will be required (i.e., will ground forces have the same networking requirements as company level units, etc.), what standards will be used, etc. In essence, we know that we need and will continue to need networking capabilities in ever increasing quantities. Another way to put our (the military as a whole) current situation is we do not have a clear definition of what our combined, specific requirements are.

Once specific requirements are determined, we must focus on how to employ the systems developed. An example of employment from TALISMAN SABER 07 is the question of "usage" for a high bandwidth system in the field. While every local commander and captain admitted that they could absolutely use a high bandwidth data system in the field, when asked what they would use it for, the response was almost always "…good question." This answer showed a lack of overall understanding of what the actual data needs of troops in the field and vessels afloat are in an overall military

[19] Assistant Secretary of Defense Networks and Integration Policy Memorandum, Subject: Use of Commercial Wireless Local Area Network Devices, Systems, and Technologies in the Department of Defense Global Information Grid, Dated: June 2, 2006.

network information system that connects geographically disparate commanders and troops together in a virtual battlefield where boundaries become geographic in nature only.

VI. CONCLUSION

The digital age has caused a paradigm shift of how we view, treat, and value information on a scale never before seen. As the military races to catch up to the advancements made in the commercial realm of information sharing, knowledge management, and information superiority, several operational concepts have developed to help guide development of military information systems. Chief among these concepts is the concept of Network Centric Warfare (NCW). Network Centric Warfare provides a conceptual view of a military which harnesses the power of information technology to provide unparalleled information sharing and processing in order to provide military commanders at all levels a complete and timely common operational picture (COP) of any area of operation in the world. Justifiably NCW only provides a conceptual view of an interconnected military, services must develop systems which best fit their operations needs while maintaining interoperability between the service specific information systems.

Since the development of the NCW concept each service has developed its own conceptual architecture of NCW. The Navy's vision of NCW is embodied in the FORCEnet concept; the Army's vision is LandWarNet, etc. What binds the visions together is the common use of IP-based communications, satellite communications, and the harnessing of the exponential growth of information systems. Interconnecting all of the service visions together is the DoD's Global Information Grid (GIG). This system is the backbone of the DoD's current and future plans for NCW operations. While the land component of the GIG has been upgraded to provide bandwidth of up to 10 Gbps, the space segment of the network has been slow up catch up to the information needs of remote, mobile units on the tactical edge of military operations.

Understandably the space segment of the GIG will lag behind the advances of the terrestrial segment. It takes years to design, build, and deploy new satellite systems that will have the ability to meet the information transfer needs of remote units operating in an NCW. However, as new information systems and COP applications are rapidly developed, their effectiveness is threatened by the limited bandwidth offered by current military satellite communications which are already overburdened by current communication requirements. Simply put, over-reliance on satellite communications, especially in intra-operational area communications threatens to delay full implementation of NCW.

On the level of the ground soldier and small unit conducting remote operations, satellite communications may not be a viable option. As an example in the Marine Corps concept of Distributed Operations (DO), each marine carries a portable computational device which is inter-networked with every other marine in the DO platoon. In this case, satellite communications is not a viable solution to individually connect each marine. In cases such as this, wireless terrestrial digital communications is the only viable solution.

Cases such as the DO example are acknowledged by each service in their conceptual architectures and addressed on a very basic level. In most cases the inter-connection of the individual unit is shown as a lighten bolt with no explanation as to what that solution is, or it is shown as a JTRS tactical data link. In either case, the solution is inadequate. In the case of the “magic lightening bolt” is implies that no solution has been discovered. If there is no interconnection between the applications, the applications are ineffective. In the case of diagrams illustrating JTRS tactical data links, despite billions of dollars and years of development the systems is still not ready for fielding on an operational basis. With this in mind, a commercially available solution should be sought.

On a larger scale, naval battle groups can be viewed in a similar light as platoon-based communications. From a purely technical point of view there is little difference between the two. However, in the case of a naval battle group, the need for information transfer is exponentially greater than that of a platoon on the shore. Unfortunately, while each ship in a battle group may be outfitted with satellite communications, they face significant bandwidth restrictions based on the design and capability of the satellite systems that are used which limit the amount of information that can be shared among them.

As a potential solution to both intra-battle group (IBG) and shored-based communications, this research proposed a tactical network based on the IEEE Std 802.16

protocol to supplement satellite communications and to act as a primary means for intra-group data communications. This tactical network architecture breaks data communications within the groups into a segmented network which interconnects the individual networks of the units using the concept of a radio-WAN. This design facilitates intra-group data communications without the use of satellite communications while allowing for the group to connect to the GIG using existing satellite communications. The net effect of this tactical network design is the reduction of bandwidth requirements for intra-group communication, facilitation of high bandwidth communications within the groups, and the enablement of NCW operations within that group; it is a potential solution to the “magic lightening bolt” shown on conceptual diagrams of NCW.

This research builds on previous research efforts pertaining to military use of wireless data communications based on IEEE Std 802.16. Through analysis of the IEEE Std 802.16 protocol, field experiments, and careful analysis of previous research, this research effort demonstrates the efficacy of wireless communications based on the IEEE 802.16 protocol in meeting IBG and shored based data communication needs. All of the equipment used during this research effort is commercially available and readily obtainable by military organizations. As was illustrated by the author, a typical battlegroup could be outfitted with a tactical network that is compatible with existing program of record shipboard networks using wireless radios based on IEEE 802.16 technology for approximately $100,000. This interoperability with IP-based communications systems and the cost effectiveness of the systems also provide an affordable and highly effective means of communicating with our coalition partners.

As was demonstrated by this research, the IEEE Std 802.16 protocol already meets, or facilitates the achievement, of all of the desired characteristics of a tactical network. Admittedly this research does note minor weaknesses in the protocol. However, with focused research by the military, any deficiencies noted by this research can easily be remedied through modification of the protocol or through additional security measures already in existence.

Focus on wireless communications based on the IEEE 802.16 protocol is important, however, attention must also be paid to supporting technology in order to make a tactical network based on IEEE 802.16 even more feasible. As was discussed in detail by this research, antenna technology is a critical factor in implementing a stable and reliable IEEE Std 802.16 based radio-WAN. While antennas are commercially available that are suitable for implementing a limited tactical network, there is no current commercial demand for the antenna systems required to fully implement a tactical network based on IEEE 802.16 technology. In order for commercial antenna manufacturers to invest in the development of advanced antennas, there must be a demand for the product; in this case this demand must be generated by the military.

From an architectural point of view, the tactical network proposed by the author provides a means of interconnecting units of a group without relying on the development of any specific application. The use of routable IP-based networks effectively decouples the application development from the development of data transmission means allowing quick and simple replacement of the tactical network when technological advancements warrant it.

In its current form the IEEE Std 802.16 protocol and communication systems based on this protocol are posed to provide military communications the enabling factor needed to provide the final link communications link necessary to bring the power of information and the capabilities of the GIG down to the level of the battegroups and the individual war fighter. Wireless data communications will provide these units the critical link that will allow the concept of NCW to revolutionize their operations. Systems based on IEEE 802.16 protocols are ready for implementation. Aside from programmatic political boundaries, there is no reason why communications based on the IEEE 802.16 protocol cannot be used to bring the full power of NCW to both the current and future battlespaces.

LIST OF REFERENCES

“Digital Battlefield: Adapted Wireless Network Systems.” Global-Defense.com. 1997. Global Defense Review. September 2007. Internet: http://www.global-defense.com/1997/digitalbattlefield.html.

“Global Information Grid (GIG) Overarching Policy.” Department of Defense Directive 8100.1. Washington, DC: September 19, 2002.

“Global Information Grid.” Defense Information Systems Agency. September 2007. Internet: http://www.disa.mil/main/ge.html.

Alberts, David, et al. Network Centric Warfare: Developing and Leveraging Information Superiority, Washington, DC: CCRP Publication Series, February 2000.

Bardwell, Joshua, and Akin, Devin. Certified Wireless Network Administrator. Berkeley, CA: McGraw-Hill/Osborne, 2005.

Bey, Christopher S. “Airborne Tactical Data Network Gateways: Evaluating EPLRS Ability to Integrate with Wireless Meshed Networks.” Naval Postgraduate School. Monterey, CA. September 2005.

Buddenburg, Rex. “Objective, Architecture and Strategy for Network-Centric: A Perspective on Mobile Communications” Naval Postgraduate School (NPS). Monterey, CA. September 2002.

Clark, Vern ADM, and Hagee, Micheal GEN. “FORCEnet: A Functional Concept for the 21st Century.” Washington, DC: 2003.

Corsano, Scott Edmund. “Joint Fires network IST Interoperability Requirements within a Joint Force Architecture.” Naval Postgraduate School. Monterey, CA. June 2003.

Craig, Clayton A. and Tsrilis, Christopher S. “Command and Control for Distributed Operations: An Analysis of Possible Technologies, Structure and Employment.” Naval Postgraduate School. Monterey, CA. June 2007.

Guice, Robert J., and Munoz, Ramon J. “IEEE 802.16 Commercial Off the Shelf (COTS) Technologies as a Complement to Objective Maneuver (STOM) Communications.” Naval Postgraduate School. Monterey, CA. September 2004.

Institute of Electrical and Electronics Engineers, Inc. “Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands.” IEEE Std 802.16e-2005.

Institute of Electrical and Electronics Engineers, Inc. “Air Interface for Fixed Broadband Wireless Access System.” IEEE Std 802.16-2004.

IXIA. Triple Play Testing with IX Chariot. IXIA Incorporated. September 2007. Internet: http://www.ixiacom.com/library/test_plans/display?skey=triple_play.

Johnson, Ballard V. and Pryor, Jameau R. “A Study of the IEEE 802.16 Mac Layer and Its Utility in Augmenting the ADNS Architecture To Provide Adaptable Intra-Strike Group High-Speed Packet Switched Data, Imagery, and Voice Communications.” Naval Postgraduate School. Monterey, CA. September 2005.

Kleinrock, Leonard. “Creating a Mathematical Theory of Computer Networks.” Operations Research. Vol. 50, No. 1, January-February 2002: 125-131.

Motorola. Motorola PTP 600 Series Bridges. Miami: Motorola, January 2007. Internet: http://www.motorolaptp.com/products/ptp600.php.

North, Rich, Norm Brown, and Len Schiavone. “Joint Tactical Radio System – Connecting the GIG to the Tactical Edge.” Washington, DC: Military Communications Conference, October 2006.

O’Rouke, Ronald. Navy Network-Centric Warfare Concept: Key Programs and Issues for Congress. Washington, DC: Congressional Reporting Service, Library of Congress, May 31, 2005.

Olsen, Randell. “Directional Ad Hoc Networking Technology.” SPAWAR Systems Center San Diego Code 80. San Diego, February 2007.

Redline Communications. RedCONNEX AN-80i Product Data Sheet. Toronto: Redline Communications. January 2007. Internet: http://www.redlinecommunications.com/news/resourcecenter/productinfo/Redconnex_brochure.pdf.

Redondo Systems, Inc. September 2007. Internet. www.redondosystems.com.

Rodriquez, William RDML. “FORCEnet Implementation.” SPAWAR Code 05, October 13, 2004. September 2007. Internet: http://www.ndia-sd.org/briefs/101304-NDIA_Rodriguez%20final.ppt.

Real-Time Innovations, Inc. September 2007, Internet, www.rti.com.

Sundaresan, Karthiskeyan and Ingram, Mary Ann. “Medium Access Control in Ad-hoc Networks with MIMO Links: Optimization Considerations and Algorithms,” in *Proc. of IEEE IC3N*, October 2005.

United States. Department of Defense. A Concept for Distributed Operations. Washington, DC: Department of the Navy, United States Marine Corps, 25 April 2005.

United States. Department of Defense. Department of Defense Information Sharing Strategy. Washington, DC: Office of the Chief Information Officer, May 2007.

United States. Department of Defense. Information and Communication Managers Course (CIN: A-202-0041C). Pensacola, FL: Department of the Navy, Chief of Naval Education and Training, August 2004.

United States. Department of Defense. Joint Technical Architecture Volume I. Washington, DC, October 2003.

United States. Department of Defense. Joint Vision: 2020. Washington, DC: Joint Chiefs of Staff, June 2000.

United States. Department of Defense. Vision, Presence, Power 2005: A Program Guide to the U.S. Navy. Washington, DC: Department of the Navy, 2005.

United States. Director, Force Transformation. Office of the Secretary of Defense. Department of Defense. The Implementation of Network-Centric Warfare. Washington, DC. January 5, 2005.

United States. Department of Defense. COTS Equipment for the Navy Shipboard UHF Digital Wideband Transmission System (DWTS). Washington, DC: Department of the Navy, Space and Naval Warfare Systems Command, July 1996.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. LtCol Carl Oros
   Naval Postgraduate School
   Monterey, California

4. Rex Buddenberg
   Naval Postgraduate School
   Monterey, California

5. Brian Steckler
   Naval Postgraduate School
   Monterey, California